
**Жизненный цикл информационной системы** — период времени, который начинается с момента принятия решения о необходимости создания информационной системы и заканчивается в момент ее полного изъятия из эксплуатации.

Понятие жизненного цикла является одним из базовых понятий методологии проектирования информационных систем.

Методология проектирования информационных систем описывает процесс создания и сопровождения систем в виде жизненного цикла (ЖЦ) ИС, представляя его как некоторую последовательность стадий и выполняемых на них процессов. Для каждого этапа определяются состав и последовательность выполняемых работ, получаемые результаты, методы и средства, необходимые для выполнения работ, роли и ответственность участников и т.д. Такое формальное описание ЖЦ ИС позволяет спланировать и организовать процесс коллективной разработки и обеспечить управление этим процессом.

Полный жизненный цикл информационной системы включает в себя, как правило, стратегическое планирование, анализ, проектирование, реализацию, внедрение и эксплуатацию. В общем случае жизненный цикл можно в свою очередь разбить на ряд стадий. В принципе, это деление на стадии достаточно произвольно. Мы рассмотрим один из вариантов такого деления, предлагаемый корпорацией Rational Software – одной из ведущих фирм на рынке программного обеспечения средств разработки информационных систем (среди которых большой популярностью заслуженно пользуется универсальное CASE-средство Rational Rose)

**Каковы критерии выбора ИС?**

**Функциональность**: Что система автоматизации может делать, или какова ее функциональность.

**Совокупная стоимость владения**: Во что обойдется приобретение системы, запуск ее в эксплуатацию и поддерживание в рабочем состоянии, т.е. какова ее совокупная стоимость владения (крайне важно знать именно общую стоимость, а не просто цену программного обеспечения).

**Гарантии успешного ввода в эксплуатацию**: Есть ли гарантии успешного завершения проекта внедрения и полноценного ввода системы в эксплуатацию (ведь система автоматизации -это целый комплекс сложных работ, а не просто коробка с программами на лазерных дисках!).

**Технические характеристики системы**: Что у системы "внутри «и, следовательно, насколько она надежна. долговечна, производительна, в конце концов, современна.

**Риски информационной безопасности в современном обществе**

За последнее время число атак на организации удвоилось. Атаки, ведущие к экстраординарному ущербу, становятся обычным явлением. Финансовый ущерб от атак возрастает и одни из самых больших потерь связаны с атаками вирусов-вымогателей. Ярким примером этого являются атаки вирусов-вымогателей WannaCry и NotPetya, затронувшие более 300 тыс. компьютеров в 150 странах мира и приведшие к финансовым потерям более 300 млн долл.

Еще одной тенденцией является увеличение количества атак на объекты критической инфраструктуры и стратегические промышленные объекты, что может привести к выводу из строя злоумышленниками систем, поддерживающих жизнеобеспечение человечества и возникновению глобальных техногенных катастроф.

Таким образом, риски информационной безопасности входят в тройку наиболее вероятных рисков (вместе с рисками природных катаклизмов и экстремальных погодных условий) и в список из шести наиболее критичных рисков по возможному ущербу (вместе с рисками применения оружия массового поражения, природными катаклизмами, погодными аномалиями и нехваткой питьевой воды). Поэтому управление рисками информационной безопасности является одним из приоритетных направлений развития организаций по всему миру и абсолютно необходимо для их дальнейшего функционирования.

Все риски, в том числе риски информационной безопасности, характеризуется двумя параметрами: потенциальным ущербом для организации и вероятностью реализации. Использование для анализа рисков совокупности этих двух характеристик позволяет сравнивать риски с различными уровнями ущерба и вероятности, приводя их к общему выражению, понятному для лиц, принимающих решение относительно минимизации рисков в организации. При этом процесс управления рисками состоит из следующих логических этапов, состав и

наполнение которых зависит от используемой методики оценки и управления рисками:

1. Определение приемлемого для организации уровня риска (риск-аппетита) – критерия, используемого при решении о принятии риска или его обработке. На основании этого критерия определяется, какие идентифицированные в дальнейшем риски будут безоговорочно приняты и исключены из дальнейшего рассмотрения, а какие подвергнуты дальнейшему анализу и включены в план реагирования на риски.
2. Идентификация, анализ и оценка рисков. Для принятия решения относительно рисков они должны быть однозначно идентифицированы и оценены с точки зрения ущерба от реализации риска и вероятности его реализации. При оценке ущерба определяется степень влияния риска на ИТ-активы организации и поддерживаемые ими бизнес-процессы. При оценке вероятности производится анализ вероятности реализации риска. Оценка данных параметров может базироваться на выявлении и анализе уязвимостей, присущим ИТ-активам, на которые может влиять риск, и угрозам, реализация которых возможная посредством эксплуатации данных уязвимостей. Также в зависимости от используемой методики оценки рисков, в качестве исходных данных для их оценки может быть использована модель злоумышленника, информация о бизнес-процессах организации и других сопутствующих реализации риска факторах, таких как политическая, экономическая, рыночная или социальная ситуация в среде деятельности организации. При оценке рисков может использоваться качественный, количественный или смешанный подход к их оценке. Преимуществом качественного подхода является его простота, минимизация сроков и трудозатрат на проведение оценки рисков, ограничениями – недостаточная наглядность и сложность использования результатов анализа рисков для экономического обоснования и оценки целесообразности инвестиций в меры реагирования на риски. Преимуществом количественного подхода является точность оценки рисков, наглядность результатов и возможность сравнения значения риска, выраженного в деньгах, с объемом инвестиций, необходимых для реагирования на данный риск, недостатками – сложность, высокая трудоемкость и длительность исполнения.
3. Ранжирование рисков. Для определения приоритета при реагировании на риски и последующей разработки плана реагирования все риски должны быть проранжированы. При ранжировании рисков, в зависимости от используемой методики, могут применяться такие критерии определения критичности, как

ущерб от реализации рисков, вероятность реализации, ИТ-активы и бизнес-процессы, затрагиваемые риском, общественный резонанс и репутационый ущерб от реализации риска и др.

4. Принятие решения по рискам и разработка плана реагирования на риски. Для определения совокупности мер реагирования на риски необходимо провести анализ идентифицированных и оцененных рисков с целью принятия относительно каждого их них одного из следующих решений:
    - Избегание риска;
    - Принятие риска;
    - Передача риска;
    - Снижение риска.

Принятое по каждому риску решение должно быть зафиксировано в плане реагирования на риски. Также данный план может содержать, в зависимости от используемой методики, следующие информацию, необходимую для реагирования на риски:

- 
    - Ответственный за реагирование;
    - Описание мер реагирования;
    - Оценка необходимых инвестиций в меры реагирования;
    - Сроки реализации этих мер.

1. Реализация мероприятий по реагированию на риски. Для реализации мер реагирования на риски ответственные лица организуют выполнение описанного в плане реагирования на риск действия в необходимые сроки.
2. Оценка эффективности реализованных мер. Для достижения уверенности, что применяемые в соответствии с планом реагирования меры эффективны и уровень рисков соответствует приемлемому для организации, производится оценка эффективности каждой реализованной меры реагирования на риск, а также регулярная идентификация, анализ и оценка рисков организации.

**На практике применяются количественный и качественный подходы к оценке рисков ИБ. В чем их разница?**

**Количественный метод**

Количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени, человекоресурсах и проч. Метод позволяет получить конкретные значения

объектов оценки риска при реализации угроз информационной безопасности.

При количественном подходе всем элементам оценки рисков присваивают конкретные и реальные количественные значения. Алгоритм получения данных значений должен быть нагляден и понятен. Объектом оценки может являться ценность актива в денежном выражении, вероятность реализации угрозы, ущерб от реализации угрозы, стоимость защитных мер и прочее.

**Как провести количественную оценку рисков?**

1.  Определить ценность информационных активов в денежном выражении.

2. Оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

Следует получить ответы на вопросы «Какую часть от стоимости актива составит ущерб от реализации каждой угрозы?», «Какова стоимость ущерба в денежном выражении от единичного инцидента при реализации данной угрозы к данному активу?».

3. Определить вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Провести анализ полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

В результате количественной оценки рисков должны быть определены:

- ценность активов в денежном выражении;
- полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;
- частота реализации каждой угрозы;
- потенциальный ущерб от каждой угрозы;
- рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

Количественный анализ рисков информационной безопасности (пример)

Рассмотрим методику на примере веб-сервера организации, который используется для продажи определенного товара. Количественный **разовый** ущерб от выхода сервера из строя можно оценить как произведение среднего чека покупки на среднее число обращений за определенный временной интервал, равное времени простоя сервера. Допустим, стоимость разового ущерба от прямого выхода сервера из строя составит 100 тысяч рублей.

Теперь следует оценить экспертным путем, как часто может возникать такая ситуация (с учетом интенсивности эксплуатации, качества электропитания и т д.). Например, с учетом мнения экспертов и статистической информации, мы понимаем, что сервер может выходить из строя до 2 раз в год.

Умножаем две эти величины, получаем, что **среднегодовой** ущерб от реализации угрозы прямого выхода сервера из строя составляет 200 тысяч рублей в год.

Эти расчеты можно использовать при обосновании выбора защитных мер. Например, внедрение системы бесперебойного питания и системы резервного копирования общей стоимостью 100 тысяч рублей в год позволит минимизировать

риск выхода сервера из строя и будет вполне эффективным решением.

**Качественный метод**

К сожалению, не всегда удается получить конкретное выражение объекта оценки из-за большой неопределенности. Как точно оценить ущерб репутации компании при появлении информации о произошедшем у нее инциденте ИБ? В таком случае применяется качественный метод.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале (0… 10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

**Как провести качественную оценку рисков:**

1. Определить ценность информационных активов.

Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива.

2. Определить вероятность реализации угрозы по отношению к информационному активу.

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

3. Определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты.

Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая). Значение возможности реализации угрозы показывает, насколько выполнимо успешное осуществление угрозы.

4. Сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы.

Для определения уровня риска можно использовать пятибалльную или десятибалльную шкалу. При определении уровня риска можно использовать эталонные таблицы, дающие понимание, какие комбинации показателей (ценность, вероятность, возможность) к какому уровню риска приводят.

5. Провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска.

Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

6. Разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

**Какой метод оценки рисков выбрать?**

Целью обоих методов является понимание реальных рисков ИБ компании, определение перечня актуальных угроз, а также выбор эффективных контрмер и средств защиты. Каждый метод оценки рисков имеет свои преимущества и недостатки.

Количественный метод дает наглядное представление в деньгах по объектам оценки (ущербу, затратам), однако он более трудоемок и в некоторых случаях неприменим.

Качественный метод позволяет выполнить оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгод от внедрения СЗИ.

Выбор метода следует делать исходя из специфики конкретной компании и задач, поставленных перед специалистом.