**Тема 9: "РАЗРАБОТКА КОРПОРАТИВНОЙ МЕТОДИКИ АНАЛИЗА РИСКОВ"**

***9.1 Постановка задачи***

Анализ информационных рисков позволяет эффективно управлять информационной безопасностью предприятия. Для этого в начале работ по анализу рисков необходимо определить, что именно подлежит защите на предприятии и воздействию каких угроз оно подвержено, а затем выработать рекомендации по практике защиты. Обсудим теперь, как разработать свою собственную методику анализа и управления информационными рисками компании.

Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Одна из важнейших задач в рамках такой защиты информации - обеспечение ее целостности и доступности. Часто забывают, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин: сбоев оборудования, ведущих к потере или искажению информации; физических воздействий, в частности в результате стихийных бедствий; ошибок в программном обеспечении (в том числе из-за недокументированных возможностей). Поэтому под термином «атака» будем понимать воздействия на информационные ресурсы не только человеческие, но и окружающей среды, в которой функционирует система обработки информации предприятия.

Анализ риска можно проводить согласно методике по сценарию, представленному на рис. 14.

Каждый из шести этапов анализа риска должен быть конкретизирован.

На первом и втором этапах выявляются сведения, составляющие для предприятия коммерческую тайну, которые предстоит защищать.

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия. В связи с этим необходимо еще раз подчеркнуть, что степень информационной безопасности определяется не только (а может быть и не столько) средствами и способами защиты, но и особенностями построения КИС. И когда говорят о КИС в защищенном исполнении, речь идет прежде всего о выборе такой архитектуры (топологии) системы обработки информации, расположения средств обработки конфиденциальной информации и способов ее хранения и передачи, которые существенно уменьшат число возможных точек доступа к информации.

Третий этап анализа риска - построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС.



***Рис.14. Сценарий анализа информационных рисков компании***

Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

Анализ способов защиты всех возможных точек атак соответствует целям защиты, и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств (четвертый этап).

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей находятся вероятности реализации угроз по каждой из возможных точек атак.

На заключительном этапе производится оценка ущерба организации в случае реализации каждой из атак. Эти данные вместе с оценками уязвимости позволяют получить ранжированный список угроз информационным ресурсам.

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу - это произведение вероятности нападения на ресурс, вероятности реализации угрозы и ущерба от информационного вторжения. В данном произведении могут быть использованы различные способы взвешивания составляющих.

Объединение рисков по всем ресурсам дает общую величину риска при принятой архитектуре КИС и внедренной в нее системы защиты информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, можно (за счет изменения вероятности реализации угроз) представить и рассмотреть различные значения риска. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с заданным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности также нужно определить **стратегию управления рисками** на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных – уменьшение риска путем принятия комплексной системы контрмер, включающей программно-технические и организационные меры защиты. Близким является подход, связанный с уклонением от риска. От некоторых классов рисков можно уклониться, например: вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее – бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

После того как стратегия управления рисками выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

Отметим, что выполнение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих областях, смежных с проблемой защиты информации.

***9.2 Методы оценивания информационных рисков***

В настоящее время используются различные методы оценки информационных рисков отечественных компаний и управления ими. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

1) Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса.

2) Оценивание возможных угроз.

3) Оценивание существующих уязвимостей.

4) Оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы. При этом информационные риски компании зависят от:

- показателей ценности информационных ресурсов;

- вероятности реализации угроз для ресурсов; эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

- привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);

- возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);

- техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;

- степенью легкости, с которой уязвимость может быть использована.

***9.3 Табличные методы оценки рисков***

В настоящее время известно множество табличных методов оценки информационных рисков компании. Важно, чтобы компания выбрала для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты. Рассмотрим несколько примеров подобных методов, рекомендованных стандартами в области информационной безопасности, и методические рекомендации к ним. Важно, что в этих методах количественные показатели имеющихся или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть путем определения затрат на их приобретение или восстановление. Если обнаружится, что к какому-либо прикладному программному обеспечению предъявляются особые требования к конфиденциальности или целостности, например исходный текст ПО обладает высокой коммерческой ценностью, то оценка этого ресурса производится в стоимостном выражении по той же схеме, что и для информационных ресурсов.

Количественные показатели информационных ресурсов рекомендуется оценивать по результатам опросов сотрудников компании - владельцев информации, то есть должностных лиц компании, которые в состоянии определить ценность информации, ее характеристики и степень критичности исходя из фактического положения дел. На основе результатов опроса оцениваются показатели и степень критичности информационных ресурсов в случае несанкционированного ознакомления с конфиденциальной информацией, нарушения ее целостности или доступности.

**Пример оценки рисков по двум факторам**

В таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учетом показателей уязвимостей. На первом шаге оценивается негативное воздействие по заранее определенной шкале, например от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка В в табл. 1).

На втором шаге по заданной шкале, например от 1 до 5, оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения (В х С). Необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) шкал измерения показатель риска, соответствующий ситуации В = 1, С = 3, совсем не обязательно эквивалентен случаю В = 3, С = 1. Соответственно, должна быть разработана методика оценивания показателей рисков применительно к конкретной организации.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

В рассматриваемом примере для наименьшего негативного воздействия и для наименьшей возможности реализации угрозы выбран показатель 1.

*Таблица 1. Ранжирование рисков*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Дескриптор угрозы** | **Показатель** | **Возможность негативного воздействия (ресурса)** | **Показатель риска реализации угрозы (субъективная оценка)** | **Ранг риска** |
| Угроза А  | 5 | 2 | 10 | 2 |
| Угроза В  | 2 | 4 | 8 | 3 |
| Угроза С  | 3 | 5 | 15 | 1 |
| Угроза D  | 1 | 3 | 3 | 5 |
| Угроза Е  | 4 | 1 | 4 | 4 |
| Угроза F | 2 | 4 | 8 | 3 |

Данная процедура позволяет сравнивать и ранжировать угрозы с различными негативными воздействиями и вероятностями реализации. В случае необходимости дополнительно могут приниматься во внимание стоимостные показатели.

**Разделение рисков на приемлемые и неприемлемые**

Другой способ оценивания рисков состоит в разделении их только на приемлемые и неприемлемые риски. Подход основывается на том, что количественные показатели рисков служат лишь для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, матрица может иметь вид табл. 2.

*Таблица 2. Разделение рисков на приемлемые и неприемлемые*

|  |  |
| --- | --- |
| **Показатель ценности ресурса**  | **Показатель возможности реализации угрозы** |
| 0 | 1 | 2 | 3 | 4 |
| 0 | Д | Д | Д | Д | Н |
| 1 | Д | Д | Д | Н | Н |
| 2 | Д | Д | Н | Н | Н |
| 3 | Д | Н | Н | Н | Н |
| 4 | Н | Н | Н | Н | Н |

Вопрос о том, как провести границу между приемлемыми и неприемлемыми рисками, остается на усмотрение аналитика, подготавливающего данную таблицу, и руководящих специалистов в области информационной безопасности.

**Пример оценки рисков по трем факторам**

По каждой группе ресурсов, связанной с данной угрозой, оценивается уровень угрозы (вероятность реализации) и уровень уязвимости (степень легкости, с которой реализованная угроза способна привести к негативному воздействию). Оценивание производится в качественных шкалах.

Сначала определим уровни угроз, уязвимостей, тяжести последствий и рисков.

Уровни угроз:

- низкий (Н) - реализация данной угрозы маловероятна, за последние два года подобных случаев не зафиксировано;

- средний (С) - угроза может реализоваться в течение одного года с вероятностью около 0,3;

- высокий (В) - угроза, скорее всего, реализуется в течение года и, возможно, не один раз.

Уровни уязвимостей:

- низкий (Н) - защищенность системы очень высока, реализация угроз почти никогда не приводит к происшествию;

- средний (С) - защищенность системы средняя, реализация около 30% угроз приводит к происшествию;

- высокий (В) - защищенность системы низкая, реализация угрозы практически всегда приводит к происшествию.

*Показатель негативного воздействия (тяжесть последствий)*

Используем введенную в теме 2 классификацию последствий:

1) Незначительные (менее $100).

2) Маленькие (менее $1000).

3) Умеренные (менее $10 000).

4) Серьёзные (существенное негативное влияние на бизнес).

5) Критические (катастрофическое воздействие, возможно прекращение функционирования системы).

*Уровни рисков*

Показатель риска измеряется по шкале от 0 до 8, уровни риска определяются следующим образом:

**1** - риск пренебрежимо мал. Ситуации, при которых событие наступает, практически исключены, а последствия незначительны, потери менее 100 долларов;

**2** - риск незначителен. Событие наступает редко, последствия (потери) находятся в допустимых пределах (не более 1000 долларов);

**8** - риск очень высок. Событие, скорее всего, наступит, и последствия будут катастрофическими (возможно полное прекращение деятельности организации).

Примером таблицы, с помощью которой задается значение уровня риска в зависимости от уровней угроз и уязвимостей при фиксированной стоимости потерь (Умеренные), является табл. 3.

*Таблица 3. Определение уровня риска в зависимости от уровней угроз и уязвимостей*

|  |
| --- |
| Уровень угрозы |
| низкий | средний | высокий |
| Уровни уязвимости | Уровни уязвимости | Уровни уязвимости |
| Н  | С  | В | Н  | С  | В | Н  | С  | В |
| 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |

Далее строится таблица для различных уровней потерь. Пример такой таблицы представлен ниже.

*Таблица 4. Определение риска в зависимости от трех факторов*

|  |  |
| --- | --- |
| Степень серьезности происшествия (цена потери)  | Уровень угрозы |
| низкий | средний | высокий |
| Уровни уязвимостей | Уровни уязвимостей | Уровни уязвимостей |
|  | Н | С | В | Н | С | В | Н | С | В |
| Незначительные | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| Маленькие | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| Умеренные | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| Серьёзные | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| Критические | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

***9.4 Методика анализа рисков Microsoft***

В качестве возможного примера корпоративной методики анализа рисков рассмотрим методику компании Microsoft.

В методике риск определяется как возможность понести убытки из-за нарушения безопасности сети изнутри или извне. Управление рисками предприятия в сфере информационной безопасности требует выполнения четырех этапов:

1) Распознавание (идентификация) рисков.

2) Определение размера риска.

3) Разработка плана управления рисками.

4) Текущий контроль и управление рисками.

При ограниченном времени для идентификации рисков рекомендуется применять методики получения сведений от экспертов, в частности метод «мозгового штурма». Для каждого выявленного риска требуется оценить его стоимость (то есть определить ущерб в том случае, если рассматриваемое нежелательное событие произошло) и вероятность возникновения риска.

Оценка для каждой из угроз может производиться следующими способами:

- с использованием группы нападения - имитируется атака на систему группой специалистов;

- методом накопления идей - создается группа сотрудников и/или консультантов, которые обсуждают возможные риски и предлагают контрмеры;

путем применения формальных оценок угроз, методов управления рисками и интеграции защитных мер.

Предлагаемая Microsoft стратегия оценки рисков включает следующие этапы:

- определение допустимого уровня рисков (то есть того уровня рисков, который приемлем);

- оценка вероятности возникновения каждого риска;

- присвоение стоимости каждому риску;

- расстановка приоритетов.

В процессе оценки для каждого риска вычисляется вероятность его возникновения и размер связанных с ним потерь. Далее используется одна из разновидностей табличной оценки рисков - строится матрица следующего вида (см. табл. 5).

*Таблица 5. Табличная оценка риска в зависимости от факторов*

|  |  |
| --- | --- |
| **Вероятность** | **Стоимость** |
| **высокая** | **средняя** | **низкая** |
| **Высокая** | Красная | Красная | Красная |
| **Средняя** | Желтая | Желтая | Желтая |
| **Низкая** | Синяя | Синяя | Синяя |

В зависимости от полученных оценок риск относится к одной из следующих групп:

- высокий риск (красная область). Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;

- существенный риск (желтая область). Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;

- умеренный риск (синяя область). В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

- незначительный риск (зеленая область). Усилия по управлению рисками в данном случае не будут играть важной роли.

На основании уровня допуска (уровня допустимых рисков), размера потенциальных потерь и вероятности их возникновения рискам назначаются приоритеты. Они служат для того, чтобы определить те риски, которые в первую очередь надо предотвратить (рекомендуется создать список десяти основных рисков, которым в первую очередь уделяется внимание), после чего составляется план по управлению рисками.

**Планирование заключается в следующем**:

- идентификации триггеров для каждого риска (триггер, или пусковое событие -идентификатор риска, реализованного или ожидаемого в скором времени);

- подготовке плана превентивных мероприятий, планов реагирования на непредвиденные ситуации и планов по уменьшению последствий каждого риска.

Выделяются четыре составные части планирования управления рисками:

- исследование;

- принятие (можно ли принять данный риск?);

- управление (можно ли сделать что-то, чтобы уменьшить риск?);

- исключение (что можно сделать, чтобы предотвратить риск или блокировать его?).

При этом исследование применяется по отношению к каждому риску, а остальные стадии могут комбинироваться. Предположим, исследование системы показало, что на предприятии установлено потенциально уязвимое приложение, причем полностью отказаться от работы с ним в данный момент невозможно. Допустим, далее данное приложение удалили на всех узлах, где это было допустимо, а на остальных, соответственно, оставили. Получается, что в отношении этого риска были выполнены следующие этапы: исследование, исключение (частичное), принятие (частичное).

Не менее важна и задача контроля рисков (отслеживания рисков), которая заключается в том, чтобы при изменении внешних или внутренних условий скорректировать сделанные ранее оценки рисков.