МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«14» сентября 2017г.

ОЦЕНКА РИСКОВ И УГРОЗ

Методические рекомендации по выполнению практических работ
для студентов укрупненных групп специальностей 10.00.00

Курск 2017

УДК 621.(076.1)

Составители: М.О. Таныгин, Е.С. Волокитина

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» А.Г. Спеваков

Оценка рисков и угроз [Текст] : методические рекомендации по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2017. – 27 с.: ил. 4, табл. 8. – Библиогр.: с. 27.

Содержат сведения и материалы по методам оценивания информационных рисков. Указывается порядок выполнения практических работ, правила оформления отчета.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,57. Уч.-изд. л. 1,42. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

МЕТОДЫ ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ. ТАБЛИЧНЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ

Цель работы:

изучить методы оценивания информационных рисков. Табличные методы оценки рисков.

Теоретический материал:

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 оценивания рисков, которые рекомендованы международными стандартами информационной безопасности, главным образом ISO 17799 (BS 7799). Существенно, что в этих рекомендуемых методах количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть при помощи определения затрат на их приобретение или восстановление количественными методами. Если обнаружится, что какое-либо прикладное программное обеспечение имеет особые требования к конфиденциальности или целостности, например, исходный текст имеет высокую коммерческую ценность, 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 могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий вплоть до

рассмотрения потенциальных воздействий на бизнес-деятельность компании при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении. При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов компании, учитывающих:

- безопасность персонала;
- разглашение частной информации;
- требования по соблюдению законодательных и нормативных положений;
- ограничения, вытекающие из законодательства;
- коммерческие и экономические интересы;
- финансовые потери и нарушения в производственной деятельности;
- общественные отношения;
- коммерческая политика и коммерческие операции;
- потеря репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные - где количественные оценки по ряду причин затруднены. При этом наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных для этих целей балльных шкалах подобной той, которая приводится далее: четырех балльная шкала от 1 до 4 баллов.

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанных с ним группе ресурсов оцениваются вероятностью реализации угроз уровни угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию. Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале "высокий - низкий". Необходимую информацию собирают, опрашивая ТОР-менеджеров компании, сотрудников коммерческих, технических, кадровых и сервисных служб,

выезжая на места и анализируя документацию компании. Рассмотрим пример.

Пример.

Проведем анализ следующих типов угроз:

- умышленные несанкционированные действия людей;
- непредвиденные случайности;
- ошибки со стороны персонала;
- аварии оборудования, программного обеспечения и средств связи.

Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оцениваются при помощи таблицы, аналогичной таблице 1

Таблица 1. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей

Показатель ценности ресурса (на каждую угрозу и ресурс)	**Уровень угрозы (оценка вероятности ее осуществления)**								
	Низкий			**Средний**			**Высокий**		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Количественный показатель риска определяется в шкале от 1 до 8. Соответствующие значения заносятся в таблицу. Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Если существует уязвимость без связанной с ней угрозы, или существует угроза, несвязанная с какими-либо уязвимыми местами, то рисков нет. Но и в этом случае следует предусмотреть изменение положения дел. Каждая строка в таблице определяется показателем ресурса, а каждый столбец - степенью опасности угрозы и уязвимости. Например,

ресурс имеет показатель 3, угроза имеет степень "высокая", а уязвимость - "низкая". Показатель риска в данном случае будет 5. Размер таблицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий ценности ресурсов, может быть изменен в соответствии со спецификой конкретной компании.

Описанный подход определяется классификацией рассматриваемых рисков. После того, как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. Эта мера в дальнейшем позволит легко повторить последующее оценивание рисков компании.

Ранжирование угроз

В матрице или таблице можно наглядно отразить связь между угрозами, негативными воздействиями и возможностями реализации. Для этого нужно выполнить следующие шаги. На первом шаге оценить негативное воздействие по заранее определенной шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка b в таблице). На втором шаге по заранее заданной шкале, например, от 1 до 5, оценить реальность реализации (колонка c в таблице) каждой угрозы (колонка a в таблице). На третьем шаге вычислить показатель риска при помощи перемножения чисел в колонках b и c, по которому и производится ранжирование угроз (колонка e). В этом примере (Таб. 2) для наименьшего негативного воздействия и для наименьшей реальности реализации выбран показатель 1.

Таблица 2. Ранжирование угроз

Описание угрозы (a)	**Показатель негативного воздействия (b)**	**Реальность реализации угрозы (c)**	**Показатель риска (d)**	**Ранг угрозы(e)**
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4

Таблица 2. Ранжирование угроз

Описание угрозы (a)	**Показатель негативного воздействия (b)**	**Реальность реализации угрозы (c)**	**Показатель риска (d)**	**Ранг угрозы(e)**
Угроза F	2	4	8	3

Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и возможностями реализации. В определенных случаях дополнительно могут потребоваться стоимостные показатели.

Оценивание показателей частоты повторяемости и возможного ущерба от риска

Рассмотрим пример оценки негативного воздействия угрозы. Эта задача решается при помощи оценивания двух значений: ценности ресурса и частоты повторяемости риска. Перечисленные значения определяют показатель ценности для каждого ресурса. Вначале каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам. После того, как баллы всех ресурсов анализируемой корпоративной системы будут просуммированы, определяется количественный показатель риска для системы. Далее оценивается показатель частоты повторяемости. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой может быть использована уязвимость. В результате получается таблица, аналогичная таблице 3.

Таблица 3. Показатель частоты повторяемости.

Уровень угрозы								
Низкий			**Средний**			**Высокий**		
Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Затем определяется показатель пары ресурс/угроза. На каждую пару ресурс/угроза составляется таблица (см. таб. 4.), в которой суммируются показатели ресурса и угрозы.

Таблица 4. Показатели пары ресурс/угроза.

Показатель ресурса	**Показатель частоты**				
	0	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3=2+1	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

На заключительном этапе суммируются все итоговые баллы по всем ресурсам системы и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Разделение рисков на приемлемые и неприемлемые

Дополнительный способ оценивания рисков состоит в разделении их только на допустимые и недопустимые. Возможность применения подобного подхода основывается на том, что количественные показатели рисков используются только для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Таблица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, может быть использована таблица 5.

Таблица 5. Разделение рисков на приемлемые и неприемлемые.

Показатель ресурса	**Показатель частоты**				
	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

При этом вопрос о том, как провести границу между допустимыми и недопустимыми рисками, как правило, предлагается решить TOP-менеджерам, ответственным за организацию информационной безопасности компании

Задание:

Промоделировать применение табличных методов оценки рисков.

Список дополнительной литературы:

Справочно-поисковая система «Консультант Плюс»;

Справочно-поисковая система «Гарант»

ОЦЕНКА РИСКОВ ПО ДВУМ ФАКТОРАМ

Цель работы

Изучить методы оценивания информационных рисков. Табличные методы оценки рисков.

Теоретический материал:

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 оценивания рисков, которые рекомендованы международными стандартами информационной безопасности, главным образом ISO 17799 (BS 7799). Существенно, что в этих рекомендуемых методах количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть при помощи определения затрат на их приобретение или восстановление количественными методами. Если обнаружится, что какое-либо прикладное программное обеспечение имеет особые требования к конфиденциальности или целостности, например, исходный текст имеет высокую коммерческую ценность, 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 могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий вплоть до рассмотрения потенциальных воздействий на бизнес-деятельность

компании при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении. При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов компании, учитывающих:

- безопасность персонала;
- разглашение частной информации;
- требования по соблюдению законодательных и нормативных положений;
- ограничения, вытекающие из законодательства;
- коммерческие и экономические интересы;
- финансовые потери и нарушения в производственной деятельности;
- общественные отношения;
- коммерческая политика и коммерческие операции;
- потеря репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные - где количественные оценки по ряду причин затруднены. При этом наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных для этих целей балльных шкалах подобной той, которая приводится далее: четырех балльная шкала от 1 до 4 баллов.

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанных с ним группе ресурсов оцениваются вероятностью реализации угроз уровни угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию. Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале "высокий - низкий". Необходимую информацию собирают, опрашивая TOP-менеджеров компании, сотрудников коммерческих, технических, кадровых и сервисных служб,

выезжая на места и анализируя документацию компании. Рассмотрим пример.

Пример оценки рисков по двум факторам.

1. В таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учетом показателей уязвимостей.
2. На первом шаге оценивается негативное воздействие по заранее определенной шкале, например от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка B в табл. 4).
3. На втором шаге по заданной шкале, например от 1 до 5, оценивается вероятность реализации каждой угрозы.
4. На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения (B × C). Необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) шкал измерения показатель риска, соответствующий ситуации B = 1, C = 3, совсем не обязательно эквивалентен случаю B = 3, C = 1. Соответственно, должна быть разработана методика оценивания показателей рисков применительно к конкретной организации.
5. На четвертом шаге угрозы ранжируются по значениям их фактора риска.
6. В рассматриваемом примере для наименьшего негативного воздействия и для наименьшей возможности реализации угрозы выбран показатель 1.
7. Таблица 6. Ранжирование рисков

Дескриптор угрозы	Показатель	Возможность негативного воздействия (ресурса)	Показатель риска реализации угрозы (субъективная оценка)	Ранг риска
Угроза A				
Угроза B				
Угроза C				
Угроза D				

Угроза E				
Угроза F				

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

9. Разделение рисков на приемлемые и неприемлемые

10. 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.

11. Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, матрица может иметь вид табл. 7.

12. Таблица 7. Разделение рисков на приемлемые и неприемлемые

Показатель ценности ресурса	Показатель возможности реализации угрозы				
	Д	Д	Д	Д	Н
	Д	Д	Д	Н	Н
	Д	Д	Н	Н	Н
	Д	Н	Н	Н	Н
	Н	Н	Н	Н	Н

13. 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.

Задание:

Промоделировать применение методов рисков по двум факторам.

Список дополнительной литературы:
Справочно-поисковая система «Консультант Плюс»;
Справочно-поисковая система «Гарант»;

РАЗДЕЛЕНИЕ РИСКОВ НА ПРИЕМЛЕМЫЕ И НЕПРИЕМЛЕМЫЕ. ОЦЕНКА РИСКОВ ПО ТРЕМ ФАКТОРАМ

Цель работы

Целью данной лабораторной работы является обучение разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам.

Теоретический материал:

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 оценивания рисков, которые рекомендованы международными стандартами информационной безопасности, главным образом ISO 17799 (BS 7799). Существенно, что в этих рекомендуемых методах количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть при помощи определения затрат на их приобретение или восстановление количественными методами. Если обнаружится, что какое-либо прикладное программное обеспечение имеет особые требования к конфиденциальности или целостности, например, исходный текст имеет высокую коммерческую ценность, 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 могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных

ресурсов для наихудшего варианта развития событий вплоть до рассмотрения потенциальных воздействий на бизнес-деятельность компании при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении. При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов компании, учитывающих:

- безопасность персонала;
- разглашение частной информации;
- требования по соблюдению законодательных и нормативных положений;
- ограничения, вытекающие из законодательства;
- коммерческие и экономические интересы;
- финансовые потери и нарушения в производственной деятельности;
- общественные отношения;
- коммерческая политика и коммерческие операции;
- потеря репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные - где количественные оценки по ряду причин затруднены. При этом наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных для этих целей балльных шкалах подобной той, которая приводится далее: четырех балльная шкала от 1 до 4 баллов.

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанных с ним группе ресурсов оцениваются вероятностью реализации угроз уровни угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию. Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале "высокий - низкий". Необходимую информацию собирают, опрашивая TOP-менеджеров компании, сотрудников

коммерческих, технических, кадровых и сервисных служб, выезжая на места и анализируя документацию компании. Рассмотрим пример.

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 такую классификацию последствий:

1) Negligible (менее $100).
2) Minor (менее $1000).
3) Moderate (менее $10 000).
4) Serious (существенное негативное влияние на бизнес).
5) Critical (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 (Moderate), является табл. 8.

Таблица 8. 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

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

Задание:

Промоделировать применение методов рисков по трем факторам.

Список дополнительной литературы:

Справочно-поисковая система «Консультант Плюс»;

Справочно-поисковая система «Гарант»;

МЕТОДИКА АНАЛИЗОВ РИСКОВ MICROSOFT

Цель работы

Изучить методики анализа рисков Microsoft.

Требования к выполнению задания:

Чтобы определить количественные характеристики, необходимо выполнить следующие задачи.

- **Задача 1.** Сопоставить каждому классу активов в организации денежную стоимость.
- **Задача 2.** Определить стоимость актива для каждого риска.
- **Задача 3.** Определить величину ожидаемого разового ущерба.
- **Задача 4.** Определить ежегодную частоту возникновения (ЕЧВ).
- **Задача 5.** Определить ожидаемый годовой ущерб (ОГУ).

Примечание. Задачи, решаемые в ходе количественной оценки рисков безопасности, схожи с операциями, используемыми в страховании для оценки стоимости актива и рисков и соответствующего страхового покрытия. На момент составления данного документа политики страхования для рисков информационной безопасности только начали появляться. Когда страховые компании накопят больше опыта в оценке рисков информационной безопасности, страховые таблицы для информационной безопасности и подобные им средства станут важным подспорьем в количественной оценке рисков.

Задача 1. Сопоставление денежной стоимости классам активов

Используя определения для классов активов, которые описаны в разделе, посвященном тематическому сбору данных, начните количественную оценку активов, соответствующих описанию класса ВВБ. Это позволит группе управления рисками безопасности в первую очередь сосредоточить усилия на активах, которые наиболее важны для организации. Для каждого актива определите денежную стоимость с точки зрения его материальной и нематериальной ценности для организации. Оценивая общую

стоимость влияния для каждого актива, используйте следующие категории.

- Стоимость замены.
- Затраты на обслуживание и поддержание работоспособности.
- Затраты на обеспечение избыточности и доступности.
- Репутация организации (репутация на рынке).
- Эффективность работы организации.
- Годовой доход.
- Конкурентное преимущество.
- Внутренняя эффективность эксплуатации.
- Правовая и регулятивная ответственность.

Примечание. Рабочая книга SRMGTool3-Detailed Level Risk Prioritization содержит рабочий лист, упрощающий данный процесс.

Определив денежные оценки для каждой категории, просуммируйте полученные значения, чтобы определить общую оценку актива. Повторите данный процесс для всех активов, представленных в классе ВВБ. В результате получится перечень активов с указанием их приоритетов и приблизительной оценки их денежной стоимости для организации. Повторите этот процесс для каждого актива в классах СВБ и НВБ.

Для каждого класса активов выберите одно денежное значение, которое будет представлять ценность класса активов. Консервативный подход состоит в выборе минимальной стоимости актива в каждом классе. Выбранное значение будет использоваться для представления ценности актива исходя из класса актива, выбранного заинтересованными лицами в процессе обсуждения собранных данных. Данный подход упрощает задачу выбора денежной стоимости каждого актива за счет использования классов активов, выбранных в ходе обсуждения собранных данных.

Примечание. Еще один подход к определению стоимости активов основан на сотрудничестве с группой управления финансовыми рисками, у которой должны быть страховые оценки и информация о страховом покрытии для соответствующих активов.

Использование существенности

Если выбор классов активов на основе рассмотренного выше метода вызывает затруднения, можно воспользоваться рекомендациями, связанными с определением существенности в финансовых отчетах, которые публикуются зарегистрированными на бирже компаниями США. Понимание этих принципов может помочь организации при выборе высокой стоимости актива для количественной оценки.

Совет по стандартам финансового учета (FASB) США выдвигает следующее требование к финансовым отчетам компаний, зарегистрированных на бирже: «Положения настоящего отчета не должны использоваться для несущественных элементов».

Необходимо помнить об этом, поскольку FASB не имеет методик, позволяющих различать существенность и несущественность, и предостерегает против использования строгих количественных методов. Вместо этого FASB рекомендует учитывать все относящиеся к делу аспекты: «FASB отказался от стандартного подхода к уменьшению „тягостных обязанностей по принятию существенных решений“ в пользу подхода, учитывающего все относящиеся к делу аспекты».

Несмотря на отсутствие конкретных формул, Комиссия по ценным бумагам и биржам в Бюллетене Комиссии по ценным бумагам и биржам № 99 подтвердила применение общего правила ссылок в государственном бухгалтерском учете для упрощения поиска существенных искажений. Дополнительные сведения см. на веб-странице www.sec.gov/interps/account/sab99.htm. В случае применения указанного выше общего правила ссылок для показателей финансовой отчетности используется величина 5%. Например, одним из способов оценки существенности чистого дохода в размере 8 млрд. долларов США может быть подробный анализ потенциальных искажений в размере 400 млн. долларов США или набора искажений, которые могут достигать 400 млн. долларов США.

Рекомендации по использованию существенности в значительной степени зависят от конкретной организации и должны применяться только в справочных целях. Процесс управления рисками безопасности, предлагаемый корпорацией

Майкрософт, не предназначен для представления финансового положения организаций каким-либо образом.

Рекомендации по использованию существенности могут помочь при определении ценности активов класса ВВБ, однако они не помогут при оценке активов в классах СВБ и НВБ. Помните, что оценка влияния носит субъективный характер и призвана выбрать значения, отражающие особенности конкретной организации. При выборе значений для классов СВБ и НВБ рекомендуется выбирать денежное значение, отражающее особенности конкретной организации с точки зрения затрат на ИТ. Кроме того, при выборе можно исходить из текущих затрат на связанные с безопасностью элементы контроля применительно к каждому классу активов. В частности, для активов класса СВБ можно сравнить соответствующее значение с текущими денежными затратами на элементы контроля базовой сетевой инфраструктуры. Например, может потребоваться оценить общую стоимость программного обеспечения, оборудования и операционных ресурсов, необходимую для внедрения в организации антивирусных средств. Это позволяет сравнить стоимость активов с величиной известных денежных затрат в организации. Еще одним примером является то, что стоимость влияния класса СВБ может быть больше, чем текущие затраты на защиту активов с помощью межсетевых экранов.

Пример банка Woodgrove. Группа управления рисками безопасности компании Woodgrove вместе с заинтересованными лицами провела работу по определению денежной стоимости классов активов. Поскольку компания ранее не применяла управление рисками, для расчета стоимости активов было решено использовать рекомендации по определению существенности. Планируется, что после получения определенного опыта эти оценки будут пересмотрены. Компания Woodgrove ежегодно получает чистый доход в размере приблизительно 200 млн. долларов США. С учетом рекомендаций по определению существенности (из расчета 5%) классу активов ВВБ была сопоставлена стоимость 10 млн. долларов США. Проанализировав последние затраты компании Woodgrove на нужды ИТ, заинтересованные лица определили, что стоимость активов класса

СВБ составляет 5 млн. долларов США, а активов класса НВБ — 1 млн. долларов США. Эти значения были выбраны исходя из затрат на большие ИТ-проекты, использовавшиеся ранее в компании Woodgrove для обеспечения безопасности и поддержки цифровых активов. На протяжении следующего ежегодного цикла управления рисками эти значения также будут пересмотрены.

Задача 2. Определение стоимости актива

После определения стоимостей классов активов необходимо определить и выбрать стоимость каждого риска. Стоимость класса актива должна быть согласована с группой классов активов, выбранной заинтересованными лицами в ходе обсуждения собранных данных. Этот же класс используется в перечнях рисков обобщенного и детализированного уровней. Данный подход уменьшает затраты времени на обсуждение стоимости конкретных активов, поскольку стоимость класса актива определяется заранее. Помните, что процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, пытается поддерживать баланс между точностью и эффективностью.

Пример банка Woodgrove. В процессе обсуждения собранных данных финансовые данные клиентов были отнесены к классу ВВБ. Таким образом, исходя из определенной выше стоимости класса ВВБ, стоимость актива составляет 10 млн. долларов США.

Задача 3. Определение степени ожидаемого разового ущерба (ОРУ)

Следующей задачей является определение степени ущерба, который может быть причинен активу. Чтобы помочь определить степень ущерба, который может быть причинен активу (в процентах), используйте уровень подверженности воздействию, определенный в ходе обсуждения собранных данных. Полученное значение называется фактором подверженности воздействию. Это же значение используется в перечнях рисков обобщенного и детализированного уровней. Консервативный подход заключается в использовании линейной скользящей шкалы для каждого значения уровня подверженности воздействию. Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, рекомендует использовать для каждого значения

уровня подверженности воздействию 20-процентную скользящую шкалу. Эту величину можно изменять в соответствии с потребностями конкретной организации.

Последний шаг состоит в получении количественной оценки влияния путем умножения стоимости актива на фактор подверженности воздействию. В классической количественной модели это значение называется величиной ожидаемого разового ущерба (ОРУ).

На рис. 1 приведен пример простого количественного подхода. Обратите внимание, что данный пример просто разделяет класс ВВБ на две части, чтобы определить средние и низкие значения. По мере получения опыта в оценке рисков эти значения могут быть изменены.

Величина высокого влияния на деятельность = $ M			Уровень подверженности воздействию	Фактор подверженности воздействию, %
			5	100
Класс актива			4	80
Значение ВВБ	**$ M**		3	60
Значение СВБ	**$ M/2**		2	40
Значение НВБ	**$ M/4**		1	20
Оценочное значение риска =	Значение класса актива × Фактор подверженности воздействию (%) = Ожидаемый разовый ущерб			

Рис. 1. Рабочий лист анализа риска: количественная оценка ожидаемого разового ущерба (SRMGTool3)

Пример банка Woodgrove. На рис. 2. показаны значения для определения ОРУ для двух примеров риска.

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб
Риск для узла локальной сети	$ 10	4	80%	$ 8
Риск для удаленного узла	$ 10	4	80%	$ 8

Рис. 2. Определение ожидаемого разового ущерба в примере с банком Woodgrove Bank: суммы указаны в миллионах долларов (SRMGTool3)

Задача 4. Определение ежегодной частоты возникновения (ЕЧВ)

После определения ожидаемого разового ущерба необходимо определить вероятность ущерба, чтобы завершить денежную оценку риска. Общепринятый подход состоит в оценке частоты возникновения риска в будущем. В дальнейшем полученное

значение преобразуется в годичную оценку. Например, если группа информационной безопасности считает, что риск может возникнуть два раза в год, ежегодная частота возникновения (ЕЧВ) будет равна 2. Если риск может возникнуть один раз в три года, ЕЧВ будет равна одной третьей (33%, или 0,33). Чтобы получить оценку вероятности, используйте качественный подход, описанный выше при рассмотрении подробного расчета риска. Чтобы упростить определение и передачу количественной оценки ЕЧВ, воспользуйтесь рис. 3.

Качественный уровень	Описание	Диапазон ежегодной частоты возникновения	Примеры описаний
Высокий	Очень вероятно	>= 1	Влияние раз в год или чаще
Средний	Вероятно	От 0,99 до 0,33	Не менее одного раза каждые 1–3 года
Низкий	Маловероятно	< 0,33	Реже, чем один раз в 3 года

Рис. 3. Количественная оценка ежегодной частоты возникновения (SRMGTool3)

Приведенный выше рисунок может использоваться только в справочных целях. Выбор значения, представляющего ЕЧВ, должен осуществляться группой информационной безопасности.

Пример банка Woodgrove. Группа управления рисками безопасности определила, что выбранные риски имеют следующие значения ЕЧВ.

- **ЕЧВ для узлов локальной сети.** Используя качественную оценку среднего уровня вероятности, группа управления рисками безопасности определила, что данный риск может возникать один раз в два года или чаще. Таким образом, значение ЕЧВ равно 0,5.
- **ЕЧВ для удаленных узлов.** Используя качественную оценку высокого уровня вероятности, группа управления рисками безопасности определила, что данный риск может возникать один раз в год или чаще. Таким образом, значение ЕЧВ равно 1.

Задача 5. Определение ожидаемого годового ущерба (ОГУ)

Чтобы завершить количественную оценку, умножьте ежегодную частоту возникновения на величину ожидаемого разового ущерба. Полученное значение называется ожидаемым годовым ущербом (ОГУ).

Ожидаемый годовой ущерб (ОГУ) = ЕЧВ × ОРУ

Величина ОГУ характеризует потенциальные годовые убытки от риска. Хотя данный показатель может помочь в оценке ущерба заинтересованным лицам, имеющим финансовую подготовку, группа управления рисками безопасности должна напомнить, что влияние на организацию не ограничивается величиной годовых издержек — возникновение риска может повлечь за собой причинение ущерба в полном объеме.

Определив количественную оценку риска, откройте рабочий лист перечня рисков на уровне детализации, который содержит дополнительный столбец, позволяющий указать дополнительные сведения о количественной оценке и необходимые пояснения. Используйте этот столбец, чтобы при необходимости помочь обосновать количественную оценку и привести доказательства.

Пример банка Woodgrove. На рис. 4. показаны базовые расчеты по определению ОГУ для каждого примера риска. Обратите внимание, что одно изменение любого показателя может привести к значительному изменению ОГУ. Используйте соответствующие качественные данные, чтобы определить количественную оценку и обосновать сделанный выбор.

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб	Количественная оценка (ожидаемый годовой ущерб)	Количественная оценка (ожидаемый годовой ущерб)
Риск для узла локальной сети	$ 10	4	80%	$ 8	0,5	$ 4
Риск для удаленного узла	$ 10	4	80%	$ 8	1	$ 8

Рис. 4. Определение величины ожидаемого годового ущерба в примере с банком Woodgrove Bank: суммы указаны в миллионах долларов (SRMGTool3)

Заключение

Этап оценки рисков цикла управления рисками необходим для управления рисками в рамках организации. Выполняя планирование, координированный сбор данных приоритизацию, помните, что этап оценки рисков призван не только выявить риски и определить их приоритеты, но и обеспечить выполнение этих задач в сжатые сроки и с максимальной эффективностью. Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, использует комбинированный подход, который основан на применении качественного анализа для быстрого поиска рисков и выявления наиболее существенных из них и

последующем определении рисков с помощью финансовых атрибутов, полученных в ходе количественного анализа.

Помощь на этапе поддержки принятия решений

Определив приоритеты рисков для организации, группа управления рисками безопасности должна выбрать соответствующие стратегии нейтрализации риска. Чтобы помочь заинтересованным лицам в выборе решений по нейтрализации риска, группа должна разработать функциональные требования, которые помогут ограничить сферу действия стратегии нейтрализации риска для соответствующего сотрудника, ответственного за нее. Вопрос разработки функциональных требований в рамках более масштабного процесса поддержки принятия решений рассматривается в главе 5 «Поддержка принятия решений».

Задание:

Промоделировать применение метода анализа рисков Microsoft.

Список дополнительной литературы:

Справочно-поисковая система «Консультант Плюс»;

Справочно-поисковая система «Гарант»;

Microsoft Security Center of Excellence.