Практическая работа №2

КОЛИЧЕСТВЕННАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы. Изучить методики оценки рисков и необходимости защиты информационной системы. Научиться рассчитывать риски, используя количественную методику.

Краткие сведения из теории

Управление информационными рисками – системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями нормативно-правовой базы (НПБ) в области защиты информации и собственной корпоративной политики безопасности.

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека.

Основной нормативно-правовой базой являются международные стандарты ISO 17799 и ISO 13335. Согласно СТБ 34.101.1–2014 риск нарушения безопасности – это возможность реализации угрозы, которая нанесет ущерб владельцу. Так же под риском понимают сочетание вероятности события и его последствий.

Суть количественной оценки рисков сводится к поиску единственного оптимального решения из множества существующих. Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного *WWW* сайта или корпоративной *E-mail*) выбрать с учетом известных ограничений бизнес-ресурсов компании?» К количественным методикам управления рисками относятся методики *CRAMM, MethodWare* и др. Рассмотрим наиболее распространённую из них.

CRAMM. Управление рисками в методике *CRAMM* осуществляется в несколько этапов. На первом этапе инициализации – «*Initialization*» – определяются границы исследуемой информационной системы компании, состав и структура ее основных физических и информационных активов и транзакций. Первичная информация собирается в процессе бесед с менеджерами

проектов, менеджером пользователей или другими сотрудниками.

На втором этапе идентификации и оценки ресурсов – «*Identification and Valuation of Assets*» – четко идентифицируются активы и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На третьем этапе оценивания угроз и уязвимостей – «*Threat and Vulnerability Assessment*» – идентифицируются и оцениваются угрозы и уязвимости информационных активов компании. Для такой оценки и идентификации в коммерческом варианте метода *CRAMM* (профиль *Standard*, в других вариантах совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения) используется следующая совокупность критериев (последствий реализации угроз информационной безопасности): критерий 1 – ущерб репутации организации; 2 – финансовые потери, связанные с восстановлением ресурсов; 3 – дезорганизация деятельности компании; 4 – финансовые потери от разглашения и передачи информации конкурентам, а также другие критерии.

Четвертый этап анализа рисков – «*Risk Analysis*» – позволяет получить количественные оценки рисков. Эти оценки могут быть рассчитаны по формулам (1) – (4):

$$R = P_{\text{ущ}} C_{\text{ущ}}; \tag{1}$$

$$R = P_{\text{угр}} P_{\text{уяз}} C_{\text{ущ}}, \tag{2}$$

где R – величина риска в результате реализации угрозы;

$P_{\text{ущ}}$ – вероятность ущерба в результате реализации угрозы;

$P_{\text{угр}}$ – вероятность реализации угрозы;

$P_{\text{уяз}}$ – вероятность реализации уязвимости;

$C_{\text{ущ}}$ – величина ущерба в результате реализации угрозы.

Если информационный объект (ИО) подвержен нескольким (N) угрозам (критериям оценки возможного ущерба), то совокупный риск ($R_{\text{общ}}$) нанесения злоумышленниками ущерба ИО может быть представлен как

$$R_{\text{общ}} = \sum_{i=1}^{N} P_i \cdot C_i, \tag{3}$$

где C_i – цена ущерба по i-й угрозе;

P_i – вероятность ущерба i-й угрозы, выбираемый экспертами из условия

$$\sum_{i=1}^{N} P_i = 1 \cdot \tag{4}$$

На пятом этапе управления рисками – «*Risk management*» – предлагаются меры и средства уменьшения или уклонения от риска. Возможно проведение коррекции результатов или использование других методов оценки. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

На заключительной стадии *CRAMM* генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

- обеспечение безопасности на сетевом уровне;
- обеспечение физической безопасности;
- обеспечение безопасности поддерживающей инфраструктуры;
- меры безопасности на уровне системного администратора.

Порядок выполнения работы

1 Оценить риски информационного объекта по методике *CRAMM*.

2 Согласно идентифицируемым уязвимостям и угрозам в практической работе № 1 определить вероятности их реализации согласно таблицам 3 и 4. Результаты оформить в виде таблицы 5.

3 Осуществить расчет рисков согласно формулам (1), (2).

4 Рассчитать общий риск для всего предприятия по формуле (3).

5 По произведенным расчетам оценить уровень ущерба по таблице 6.

Таблица 1 – **Оценка вероятности осуществления угрозы**

Вероятность атаки	Описание	Значение вероятности
1 Очень низкая	Угроза практически никогда не произойдет	[0; 0,25)
2 Низкая	Маловероятно, что эта угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали бы на то, что это может произойти.	[0,25; 0,5)
3 Средняя	Вероятность проведения угрозы равновероятна	0,5
4 Высокая	Возможно, эта угроза осуществится (в прошлом происходили инциденты), или существует статистика или другая информация, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий	(0,5; 0,75]

5 Очень высокая	Угроза, скорее всего, осуществится. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия	(0,75; 1]

Таблица 2 – **Оценка вероятности осуществления угрозы через уязвимости**

Вероятность осуществления	Описание	Значение вероятности
1 Высокая	Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует	(0,75; 1]
2 Средняя	Уязвимость может быть использована, но существует определенная защита	[0,35; 0,75)
3 Низкая	Уязвимость сложно использовать, и существует хорошая защита	[0; 0,35)

Таблица 3 – **Результаты анализа рисков информационного объекта**

Наименование уязвимости	Наименование угрозы	Вероятность осуществления угрозы	Вероятность осуществления уязвимости	Риск, у.е.

Таблица 4 – **Оценка уровня ущерба**

Уровень ущерба	Описание
1 Малый (менее 1000 у.е.)	Незначительные потери материальных активов, которые быстро восстанавливаются, или незначительные последствия для репутации компании
2 Умеренный (от 1000 до 5000 у.е.)	Заметные потери материальных активов, или умеренные последствия для репутации компании
3 Средней тяжести (от 5000 до 10000 у.е.)	Существенные потери материальных активов или значительный урон репутации компании
4 Большой (от 10000 до 30000 у.е.)	Большие потери материальных активов и большой урон репутации компании
5 Критический (более 30000 у.е.)	Критические потери материальных активов, или полная потеря репутации компании на рынке, что делает невозможным ее дальнейшую деятельность

Содержание отчета

1 Цель работы.

2 Результаты оценки рисков по количественной методике, оформленные согласно таблице 3.

3 Вывод по работе.

Контрольные вопросы

1 Этапы количественной методики оценки рисков.
2 Стандарты, регламентирующие управление информационными рисками.
3 Что такое управление информационными рисками?
4 Суть этапа инициализации количественной методики оценки рисков.
5 Критерии оценивания угроз и уязвимостей.
6 Этап анализа рисков.
7 Основные отличия качественной методики оценки рисков от количественной?