

## ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3

### АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Цель занятия:** изучить методику анализа рисков информационной безопасности и получить практические навыки по ее применению.

#### 1 Краткие теоретические сведения

Управление информационными рисками представляет собой одно из наиболее динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача – объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под термином «управление информационными рисками» обычно понимается 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. Качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании. При этом основной НПБ являются британский стандарт *BS 7799* «Практические правила управления информационной безопасностью (ИБ)» и германский стандарт *BSI*, на основе которых были приняты международные стандарты *ISO 17799* и *ISO 13335*.

Согласно ГОСТ Р 51897-2002 риск – это сочетание вероятности события и его последствий, а величина риска может быть вычислена по формулам:

$$\text{РИСК} = \text{ВЕРОЯТНОСТЬ}_{\text{ущерба}} \cdot \text{ЦЕНА}_{\text{ущерба}} \quad (1)$$

$$\text{РИСК} = \text{ВЕРОЯТНОСТЬ}_{\text{угрозы}} \cdot \text{ВЕРОЯТНОСТЬ}_{\text{уязвимости}} \cdot \text{ЦЕНА}_{\text{ущерба}} \quad (2)$$

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

$$\text{РИСК}_{\text{общий}} = \sum_{i=1}^N p_i \cdot U_i, \quad (3)$$

где  $U_i$  –  $\text{ЦЕНА}_{\text{ущерба}}$  по  $i$ -й угрозе;

$p_i$  –  $\text{ВЕРОЯТНОСТЬ}_{\text{ущерба}}$  (весовой коэффициент)  $i$ -й угрозы, выбираемый экспертами из условия:

$$\sum_{i=1}^N p_i = 1 \quad (4)$$

Методики управления рисками делятся на количественные и качественные.

Качественные методики относительно просты, и разработаны на основе требований стандарта *ISO 17799*. К качественным методикам управления рисками относятся методики *COBRA* и *RA Software Tool*.

Методика *COBRA* представляет требования стандарта *ISO 17799* в виде тематических вопросников (*check list's*), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнес-транзакций компании. Далее введенные ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению.

Методика *RA Software Tool* позволяет выполнять оценку информационных рисков в соответствии с требованиями *ISO 17799*, а при желании в соответствии с более детальными спецификациями руководства *PD 3002* (Руководство по оценке и управлению рисками) Британского института стандартов.

Вторую группу методик управления рисками составляют *количественные методики*. Суть их сводится к поиску единственного оптимального решения из множества существующих. Чтобы прийти к такому решению, 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 веб-сайта или корпоративной электронной почты) 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* (CCTA Risk Analysis and Management Method; CCTA – Central Computer and Telecommunications Agency). 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 различными менеджерами компании.

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».

Критерий 2: «Финансовые потери, связанные с восстановлением ресурсов».

Критерий 3: «Дезорганизация деятельности компании».

Критерий 4: «Финансовые потери от разглашения и передачи информации конкурентам».

Четвертый этап анализа рисков – «Risk Analysis» – позволяет получить количественные оценки рисков. Эти оценки могут быть рассчитаны по формулам (1)-(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;
- обеспечение безопасности на уровне системного администратора.

Ключевыми определениями при анализе информационных рисков являются следующие.

Критичность реализации угрозы ( $ER$ ) – степень влияния реализации угрозы на ресурс, т.е. как сильно повлияет угроза на работу ресурса.

Вероятность реализации угрозы через данную уязвимость ( $P(V)$ ) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях.

Исходя из данных двух параметров, определяется уровень угрозы по уязвимости ( $Th$ ):

$$Th = \frac{ER}{100} \cdot \frac{P(V)}{100} \quad (5)$$

На основании значений уровней угроз по уязвимости осуществляется расчет по всем уязвимостям, по которым реализуется данная угроза ( $CTh$ ):

$$CTh = 1 - \prod_{i=1}^n (1 - Th_n) \quad (6)$$

Рассмотрим возможности методики CRAMM на примере. Пусть проводится оценка информационных рисков следующей корпоративной информационной системы, структура которой представлена на рисунке 1.

В этой схеме условно выделим следующие элементы системы:

- рабочие места (РМ), на которых операторы вводят информацию, поступающую из внешнего мира;
- почтовый сервер, на который информация поступает с удаленных узлов сети через Интернет и из ведомственных каналов связи (ВКС);
- сервер обработки, на котором установлена система управления базами данных (СУБД);
- сервер резервного копирования;
- рабочие места группы оперативного резерва;
- рабочее место администратора безопасности и администратора СУБД.

Функционирование системы осуществляется следующим образом. Данные, введенные операторами с рабочих мест и поступившие на почтовый сервер из Интернета и из ВКС, направляются на сервер корпоративной обработки данных. К этим данным

имеется доступ у группы оперативного резерва, которая анализирует их и принимает решения по передаче данных в СУБД.



Рисунок 1– Структура корпоративной информационной системы

## 2 Практическое задание

Проанализируем риски только в части информационных активов с помощью методики *CRAMM* и предложим некоторые средства контроля и управления рисками, адекватные целям и задачам бизнеса компании.

*Этап 1. Определение границ исследования.*

Для этого определяется состав и структура основных информационных активов системы. Пусть в нашем случае информационными активами системы являются:

Актив 1. Данные, поступившие за день в СУБД из Интернета.

Актив 2. Данные, поступившие за день в СУБД из ВКС.

Актив 3. Данные, поступившие за день в СУБД с РМ операторов.

Актив 4. Программное обеспечение (ПО) информационной системы.

Актив 5. Данные в СУБД.

*Этап 2. Стоимость информационных активов.*

Актив	1	2	3	4	5
Стоимость, руб.	700	500	3200	9000	500000

*Этап 3. Анализ угроз и уязвимостей.*

Пусть основными угрозами с наиболее высокими приоритетами выбраны:

Угроза 1. Проникновение из Интернета в сеть организации вредоносного программного обеспечения.

Угроза 2. Несанкционированный доступ к информационным активам сотрудника компании, завербованного конкурентами и передающего им информацию.

*Этап 4. Количественные оценки рисков.*

Пусть в результате реализации угрозы 1 наступило первое последствие «Финансовые потери, связанные с восстановлением ресурсов», причём вредоносное ПО проникало в сеть организации 6 раз в год и каждый раз повреждало на 100 % активы 1-3 и на 20 % актив 4. Актив 5 был защищён резервным копированием и повреждением его можно пренебречь.

Кроме того, в результате реализации этой угрозы наступило второе последствие «Дезорганизация деятельности компании». За 6-кратное в течение года проникновение вредоносного ПО цена ущерба по этому последствию составила 2100 руб.

Пусть в результате реализации угрозы 2 наступило первое последствие «Финансовые потери от разглашения и передачи информации конкурентам». Цена ущерба по этому последствию за год составила 17600 руб.

Кроме того, в результате реализации этой угрозы наступило второе последствие «Ущерб репутации организации». Цена ущерба по этому последствию за счёт уменьшения потока заказов и неприятностей со стороны государственных органов составила 33000 руб. за год.

Вероятность ущерба для угрозы 1 составляет 60 %, а для угрозы 2 – 40 %.

*Этап 5. Выбор методов парирования угроз.*

Пусть методом парирования угрозы 1 является закупка определённого набора программных средств (фаерволла, межсетевого экрана), а методом парирования угрозы 2 – разработка и внедрение системы назначения паролей для доступа к информационным активам. Стоимость наилучшего фаерволла – 9000 руб. Стоимость разработки и внедрения наилучшей системы назначения паролей – 2000 руб. Утверждённый годовой бюджет на информационную безопасность составляет 8000 руб.

**Задание 2.1.** Найти цену ущерба по угрозе 1.

**Задание 2.2.** Найти цену ущерба по угрозе 2.

**Задание 2.3.** Найти РИСК<sub>общий</sub>.

**Задание 2.4.** Исходя из критерия «Как, оставаясь в рамках утвержденного годового бюджета на информационную безопасность достигнуть максимального уровня защищенности информационных активов компании (минимума риска)?» требуется оптимально распределить средства годового бюджета (8000 руб.) на парирование угрозы 1 и парирование угрозы 2, считая, что для рассматриваемой корпоративной информационной системы экспертным путём установлено, что:

– недостаток каждых  $x$  % средств от стоимости наилучшего фаерволла позволяет приобрести более дешёвый фаерволл, оставляющий, однако, риск угрозы 1 в размере:

$$R_{ост.1} = R_1 \cdot \frac{x}{100} \text{ (руб.)} \quad (7)$$

где  $R_1$  – РИСК по 1-й угрозе, руб.;

– недостаток каждых  $y$  % средств от стоимости наилучшей системы назначения паролей позволяет приобрести более дешёвую систему, оставляющую, однако, риск угрозы 2 в размере:

$$R_{ост.2} = R_2 \cdot \frac{y}{100} \text{ (руб.)} \quad (8)$$

где  $R_2$  – РИСК по 2-й угрозе, руб.;

Общий риск угроз после внедрения мер должен быть минимально возможным:

$$R_{после\ внед.\ мер} = (R_{ост.1} + R_{ост.2}) \rightarrow \min \quad (9)$$

Можно выделить  $N$  способов распределения выделенных средств на парирование угроз 1 и 2, например, случай 1: на фаерволл – 8000 руб., тогда на систему назначения паролей остается – 0 руб. Отсюда определяем % недостатка средств:

$$x = \frac{9000 - 8000}{9000} = \frac{1}{9} \approx 11\%; \quad y = \frac{2000 - 0}{2000} = 1 = 100\% \quad (10)$$

Подставив полученные значения в формулы (7)-(9) находят величину общего риска после внедрения мер.

Аналогично выполняются расчеты для следующих  $N-1$  способов распределения выделенных средств, после чего выбирается минимальный общий риск угроз.

**Задание 2.5.** Оценить эффективность принятых мер безопасности (в процентах) для парирования угроз ( $EF$ ), т.е. на сколько процентов уменьшится риск до внедрения мер (риск общий) по сравнению с минимальным риском после их внедрения.

**Задание 2.6.** Найти критичность реализации угрозы 1 через уязвимость 1 ( $ER_{1/1}$ ), т.е. степень влияния однократной реализации угрозы 1 на среднюю работоспособность всех пяти информационных активов системы. Определить для выявленных угроз и уязвимостей:

- уровень угрозы 1 по уязвимости 1 ( $Th_{1/1}$ );
- уровень угрозы 1 по уязвимости 2 ( $Th_{1/2}$ );
- уровень угрозы 2 по уязвимости 1 ( $Th_{2/1}$ );
- уровень угрозы 2 по уязвимости 2 ( $Th_{2/2}$ );
- уровень угрозы 1 по всем (двум) уязвимостям ( $CTh_1$ );
- уровень угрозы 2 по всем (двум) уязвимостям ( $CTh_2$ ).

Критичность реализации угрозы 1 через уязвимость 2 составляет 20 %; угрозы 2 через уязвимость 1 – 30 %; угрозы 2 через уязвимость 2 – 40 %. Вероятности реализации угроз через каждую из уязвимостей ( $P(V)$ ) считать равновероятными, т.е. 50 %.

**Задание 2.7.** На основании полученных результатов сделать вывод о целесообразности проведения мер противодействия выявленным угрозам, и указать категории контрмер (см. страница 3), к которым можно отнести предлагаемые методы парирования из пятого этапа.

### 3 Содержание отчета

3.1 Исходные данные для расчета, содержащиеся в описании этапов 1-3.

3.2 Расчеты и результаты по заданиям 2.1-2.7 с указанием названий рассчитываемых величин и их единиц измерения.