**ПРАКТИЧЕСКИЕ ЗАДАНИЯ №2, 3**

**АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Краткие теоретические сведения**

*Информационная безопасность* – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. В такой формулировке этот термин определен в Концепции национальной безопасности Республики Беларусь, а также фигурирует в Концепции информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1.

*Угроза* информационной безопасности – потенциальная или реальная существующая возможность нанесения ущерба интересам личности, общества и государства в информационной сфере.

*Защита информации* – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

*Уязвимость* – некоторое свойство информационного объекта (информационной системы), делающее возможным возникновение и реализацию угрозы.

*Атака* – действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости*.*

Целью защиты информационного объекта (информационной системы) является противодействие угрозам безопасности. *Защищенный информационный объект (информационная система)* — это объект (система) со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

*Риск* – сочетание вероятности события и его последствий. *Информационный риск* – сочетание вероятности реализации угрозы информационной безопасности и последствий от реализации угрозы информационной безопасности.

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.

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*. Вторую группу методик управления рисками составляют количественные методики. К количественным методикам управления рисками относятся методики *CRAMM*, *MethodWare* и др.

**Практическое задание № 2**

**«Анализ рисков информационной безопасности»**

**Оценка необходимости защиты информационной системы**

**Цель:** приобретение практических навыков качественной оценки рисков информационной безопасности

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 c текущими оценками информационных рисков компании и рекомендациями по их управлению.

Методика предназначена для проведения общей и частных оценок, позволяющих руководителю организации принять обоснованное решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, от конкурентов с оценкой предстоящих расходов на защиту. Методика позволяет быстро и достаточно объективно провести экспресс-оценку необходимости защиты конфиденциальной информации и на ее основе оперативно принять соответствующее решение.

Методика состоит из двух взаимосвязанных частей. Первая часть позволяет на основе обработки результатов анкетного опроса принципиально ответить на вопрос, нужно или не нужно защищать информацию, циркулирующую на фирме, а вторая часть, в случае положительного решения первого вопроса, позволяет приближенно оценить затраты на предстоящую ЗИ.

**Перечень анкетных вопросов**

Вопросы анкеты сформулированы таким образом, что не требуют пространных ответов, а сводятся к односложным ответам «да», «нет». Заполнение анкеты не требует специальной подготовки в области ЗИ и не вызывает трудностей и больших временных затрат. Специальные знания по ЗИ учтены при разработке анкетных вопросов и при последующей обработке результатов опроса с участием специалистов по ЗИ.

Количественная оценка наличия конфиденциальной информации в организации и необходимости ее защиты получается путем математической обработки ответов на анкетные вопросы. С этой целью каждому вопросу анкеты поставлена в соответствие весовая величина, численно выражающая долевой вклад содержания вопроса в необходимость защиты конфиденциальной информации. Значения весовых коэффициентов получены экспертным методом.

При обработке результатов анкетного опроса можно получить как общую оценку необходимости защиты на фирме, так и ряд частных оценок по возможным направлениям защиты. Совокупность всех оценок позволяет руководителю, в конечном счете, принять решение о необходимости организации защиты путем проведения режимных, организационных и технических мер.

На основе анализа полученных оценок выявляются те звенья защиты, где она не обеспечена и вероятность перехвата информации конкурентом (утечка) недопустимо высока. Проведя такой анализ, руководитель организации может целенаправленно проводить работы по устранению утечки информации по выявленным направлениям.

Порядок проведения оценок и существо первой части методики заключается в следующем.

На первом этапе заинтересованная в ЗИ сторона в лице учредителя или руководителя организации заполняет анкету, отвечая на ее вопросы, приведенные в таблице 1. Ответы на вопросы анкеты в форме «да» или «нет» заносятся в графу 3 против соответствующих вопросов (см. таблица 2).

Таблица 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | | Вопросы анкеты | Долевые коэффициенты для общей оценки | | Долевые коэффициенты для частных оценок |
| 1 | | 2 | 3 | | 4 |
| Уровень конкуренции | | | | | |
| 1 | | 1) Конкурентоспособна ли Ваша продукция на внутреннем рынке? | 3,5 | | 35 |
| 2) Конкурентоспособна ли Ваша продукция на внешнем рынке? | 5,0 | | 50 |
| 3) Монопольна ли Ваша продукция на внутреннем рынке? | 1,5 | | 15 |
| Степень конфиденциальности информации, циркулирующей на фирме | | | | | |
| 2 | 1) Имеется ли информация, предназначенная только лицам верхнего звена управления, с грифом «строго конфиденциально»? | | | 11,0 | 55 |
| 2) Имеется ли информация, предназначенная ограниченному кругу лиц, выполняющих конкретные операции и задания, в части их касающаяся, с грифом «конфиденциально»? | | | 5,0 | 25 |
| 3) Имеется ли информация ограниченной доступности только работникам организации? | | | 4,0 | 20 |

Продолжение таблицы 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | | 3 | | 4 |
| Время «старения» конфиденциальности информации | | | | | |
| 3 | 1) Носит ли конфиденциальность долговременный характер (год и более)? | | 5,0 | | 50 |
| 2) Носит ли конфиденциальность кратковременный характер (месяц и более)? | | 4,0 | | 40 |
| 3) Носит ли конфиденциальность оперативный характер (до месяца)? | | 1,0 | | 10 |
| Режимные и организационные мероприятия | | | | | |
| 4 | 1) Учитываются ли интересы сохранения тайны организации при кадровом отборе верхнего звена управления? | | 3,8 | | 13 |
| 2) То же при подборе лиц, которые будут допущены к конфиденциальной информации? | | 2,7 | | 9 |
| 3) То же при кадровом отборе штатного персонала организации в целом? | | 1,5 | | 5 |
| 4) Налажен ли контроль за сохранением работниками организации коммерческой тайны? | | 1,8 | | 6 |
|  | 5) Обеспечена ли охрана организации и защита конфиденциальной документации, содержащей коммерческую тайну? | | 2,2 | | 7,4 |
|  | 6) Возможен ли доступ «недопущенных»  лиц к средствам размножения и обработки информации, отнесенной к указанным в пункте 2 категориям конфиденциальности? | | 2,3 | | 7,6 |
| 7) Возможно ли, по Вашему мнению, проникновение агента конкурирующей организации в верхнее звено управления? | | 6,0 | | 19,7 |
| 8) То же в среднее звено управления? | | 3,7 | | 12,3 |
| 9) То же в обслуживающий технику персонал? | | 2,3 | | 7,6 |
| 10) То же в персонал, выполняющий работы, прямо не связанные с конфиденциальной информацией? | | 1,5 | | 5 |
| 11) Выделено ли специальное помещение для совещаний и переговоров с деловыми партнерами? | | 2,5 | | 7,4 |
| Оснащение служебных помещений техническими средствами | | | | | |
| 5 | | 1) Проводными телефонами? | | 2,5 | 10,5 |

Продолжение таблицы 1

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
|  | 2) Переговорными устройствами (рациями)? | 1,5 | 5 |
| 3) Датчиками пожарной и охранной сигнализации? | 0,6 | 2 |
| 4) Электронными часами? | 0,8 | 2,5 |
| 5) Установками прямой телефонной связи? | 1,3 | 7 |
| 6) Телевизорами? | 1,5 | 5 |
| 7) Диктофонами? | 0,5 | 1,5 |
| 8) Радиотелефонами? | 1,5 | 7 |
| 9) Установкой оперативной (директорской) телефонной связи? | 1,5 | 7 |
| 10) Телефаксами? | 2,2 | 7,5 |
| 11) Персональными компьютерами? | 6,0 | 13,5 |
| 12) Системами видеонаблюдения? | 0,9 | 3 |
| 13) Автоматической телефонной станцией? | 4,5 | 12 |

На втором этапе с привлечением консультанта проводится анализ результатов опроса. Если ответ на вопрос соответствует увеличению опасности утечки информации, то в графе 4 табл. 3 проставляется знак «+», в противном случае проставляется знак «-».

На третьем этапе производится суммирование долевых коэффициентов графы 5, соответствующих знаку «+» по всем вопросам анкеты. Результат суммирования является общей оценкой (G) для принятия решения о необходимости защиты конфиденциальной информации на фирме в Целом. При этом если общая оценка G равна или больше 50 (G>50), то **защиту необходимо проводить по всем направлениям.** Если общая оценка G больше 20, но меньше 50 (50>G>20), то вероятность утечки информации достаточно велика и защита необходима по отдельным направлениям. Если общая оценка меньше 20 (G < 20), то **вероятность утечки информации мала и дополнительную защиту информации можно не проводить.**

На четвертом этапе проводится анализ с помощью частных оценок по всем 5 пунктам опросной анкеты. Для получения частных оценок проводят суммирование долевых коэффициентов графы 6 табл. 2, помеченных знаком «+» для каждого пункта отдельно. При этом получится пять частных оценок:

1) по пункту 1 – оценка конкурентоспособности продукции (услуг) – G1;

2) по пункту 2 – оценка степени конфиденциальности информации – G2;

3) по пункту 3 – оценка временных характеристик конфиденциальности информации – G3;

4) по пункту 4 – оценка ЗИ режимными и организационными методами – G4;

Таблица 2 – Результаты анализа ответов на вопросы анкеты

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Анкета | №  вопроса | Ответы на вопросы | Результаты анализа ответов | Долевые коэффициенты  для обшей  оценки | Долевые коэффициенты  для частных  оценок | Общая оценка | Частные оценки | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 2 | 1 |  |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 3 | 1 |  |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 | 1 |  |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 5 | 1 |  |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |

5) по пункту 5 – оценка возможности утечки информации через технические средства – G5.

Если частная оценка по каждому из пунктов 1-3 равна или больше 20 (G 1, 2, 3 > 20), то **это подтверждает необходимость ЗИ.**

Если частная оценка по каждому из пунктов 4, 5 равна или больше 20 (G 4, 5 > 20), то это указывает на необходимость проведения ЗИ режимными и организационными методами или с помощью технических средств защиты соответственно. В том случае, если частная оценка по одному из пунктов 1-3 меньше 20 (G 1, 2, 3 < 20), то **ЗИ можно не проводить.**

Таким образом, на основе проведенных оценок руководитель организации принимает решение о необходимости проведения работ по организации ЗИ.

Вполне естественно, что перед руководителем организации встает другой очень важный вопрос о предстоящих затратах на организацию ЗИ. Этот вопрос решается с помощью второй части методики.

Вторая часть методики предназначается для определения ориентировочной оценки ожидаемых затрат, связанных с защитой конфиденциальной информации. В общем случае затраты на ЗИ складываются из затрат на проведение организационно-режимных и технических мер. В свою очередь, затраты на техническую защиту складываются из затрат на проведение защиты речевой информации и на защиту других видов информации, в частности, дискретной, обрабатываемой на ПК, телеграфной, факсимильной и других видов, используемых в деятельности организации.

Затраты на режимные и организационные меры ЗИ определяются главным образом заработной платой работников режимных подразделеий (групп) обеспечивающих организацию и контроль режимных мер, повышающих безопасность информации. Расчет этих затрат полностью находится в ведении руководителя организации и затруднений не вызывает. Затраты на техническую ЗИ складываются из затрат на проведение исследований, позволяющих выявить каналы утечки информации, определить способы ее защиты и из ожидаемых затрат на реализацию технических решений защиты.

Расчет стоимости защитных мероприятий каждого из видов информации имеет некоторые особенности, но на этапе ориентировочных расчетов можно использовать методику защиты речевой информации как наиболее простой и общей. Такая методика, являющаяся второй составной частью общей методики оценки, разработана и представлена ниже. Учитывая, что методика предназначена для проведения экспресс-оценки стоимости ЗИ, позволяющей руководителю организации грубо оценить предстоящие затраты, она максимально упрощена и предусматривает проведение элементарных расчетов. С этой целью все техническое оборудование, которое может быть установлено на объекте (фирме) и через которое возможна утечка информации, условно разделено на три группы. Критерием такого деления выбрана доля (процент) затрат на защиту оборудования от стоимости самого оборудования (техники). Долевые коэффициенты (Kl, К2, КЗ) определены экспертным путем и приведены в табл. 3.

Таблица 3 – Стоимость защиты оборудования

|  |  |  |  |
| --- | --- | --- | --- |
| Группа | Перечень оборудования | Доля (процент) затрат  на защиту оборудования от утечки информации | Доля (процент) затрат на  ежегодный профилактический контроль эффективности ЗИ |
| 1 | 2 | 3 | 4 |
| 1 | проводные телефоны; переговорные устройства (рации); датчики пожарной и охранной сигнализации; электронные часы | *К*1 = 0,7∙*С*1 | *Кпроф* = (0,05…0,1)∙(*С*1+*С*2+*С*3) |
| 2 | установки прямой телефонной связи; телевизоры; диктофоны; радиотелефоны | *К*2 = 0,3∙*С*2 |
| 3 | пульты оперативной (директорской) телефонной связи до 100 номеров; телефаксы; персональные компьютеры; системы видеонаблюдения;  АТС на 100-1000 номеров | *К*3 = 0,15∙*С*3 |

*Примечание: в табл. 3. приводится расчет стоимости защиты оборудования, не предназначенного для передачи, обработки и хранения конфиденциальной информации. Стоимость защиты оборудования, предназначенного для обработки конфиденциальной информации, определяется индивидуально и может существенно превышать указанную в табл. 3.*

В таблице обозначено: *С*1, *С*2, *С*3 – суммарная стоимость технического оборудования соответствующей группы, установленного в организации. Значения стоимости образцов техники, находящихся в помещениях организации, определяются по каталогам действующих цен изготовителя данной техники (можно воспользоваться приближенными ценами из таблицы 4).

Стоимость технической защиты всего оборудования (*Стз*), состоящего из техники различных групп, определяется по формуле:

|  |  |
| --- | --- |
| *Стз* = *К*1 + *К*2 + *К*3 | (2.1) |

Примечание: в таблице 3 не приводится расчет стоимости защиты специального оборудования, используемого для передачи, обработки и хранения конфиденциальной информации. Стоимость защиты такого оборудования определяется индивидуально и может существенно превышать указанную в таблице 3.

Стоимость ежегодного профилактического контроля определяется по формуле:

|  |  |
| --- | --- |
| *Спроф* = *Кпроф* | (2.2) |

Таким образом, зная перечень и количество установленного в организации технического оборудования и его стоимость, можно без труда рассчитать общие ожидаемые затраты на ЗИ техническими средствами:

|  |  |
| --- | --- |
| *Собщ.з.* = *Стз + Сраз + Спроф* | (2.3) |

где *Сраз* – ежегодные затраты на режимные и организационные меры, которые определяются заработной платой работников службы информационной безопасности. В случае отсутствия данной службы коэффициентом можно пренебречь.

Получив такие оценки, руководитель организации принимает решение на проведение работ по защите информации.

|  |  |
| --- | --- |
| Таблица 4 – Приблизительная стоимость технических средств | |
| Наименование | Стоимость, бел. руб. |
| 1) Проводные телефоны | 60 |
| 2) Переговорные устройства (рации) | 100 |
| 3) Датчики пожарной / охранной сигнализации | 30 / 55 |
| 4) Электронные часы | 50 |
| 5) Установки прямой телефонной связи | 100 |
| 6) Телевизоры | 1000 |
| 7) Диктофоны | 50 |
| 8) Радиотелефоны | 85 |
| 9) Установки оперативной (директорской) телефонной связи | 1500 |
| 10 Телефаксы | 860 |
| 11) Персональные компьютеры | 1700 |
| 12) Системы видеонаблюдения | 850 |
| 13) Автоматические телефонные станции | 200 |

**Практическое задание**

1. Провести оценку необходимости защиты конфиденциальной информации в данной организации в соответствии с приведенной методикой. Сделать вывод о необходимости защиты информации в организации.

2. Оценить ожидаемые затраты на обеспечение безопасности информационной системы. Сделать вывод о готовности организации затратить полученную сумму на защитные мероприятия.

**Контрольные вопросы**

1. Что такое информационный риск?

2. В чем заключается задача управления информационными рисками?

3. Какие существуют методики оценки рисков и управления ими?

4. Какие этапы включает в себя методика оценки информационных рисков COBRA?

5. Как определяются общие ожидаемые затраты на ЗИ техническими средствами:

**Практическое задание № 3 «Анализ рисков информационной безопасности. Количественная оценка и управление рисками информационной безопасности»**

**Цель:** приобретение практических навыков количественной оценки рисков информационной безопасности.

Вторую группу методик управления рисками составляют количественные методики. Суть количественных методик оценки информационных рисков и управления ими сводится к поиску единственного оптимального решения из множества существующих. Наиболее популярной качественной методикой оценки информационных рисков и управления ими является методика CRAMM (от англ. CCTA Risk Analysis and Managment Method; CCTA – аббревиатура от англоязычного названия британской организации-разработчика методики: Computer and Telecommunications Agency).

Методика CRAMM включает в себя 5 этапов:

1. Инициализация (Initialization). На этом этапе необходимо определить границы исследуемой информационной системы компании, состав и структуру ее основных физических и информационных активов и транзакций. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

2. Идентификация и оценка ресурсов (Identification and Valuation of Assets). На этом этапе необходимо идентифицировать информационные активы и рассчитать их стоимость. Расчет стоимости информационных активов необходим для того, чтобы определить необходимость и достаточность используемых средств и систем защиты информации.

3. Оценка угроз и уязвимостей (Threat and Vulnerability Assessment). На этом этапе необходимо идентифицировать и оценить угрозы и уязвимости информационных активов.

4. Анализ рисков (Risk Analysis). На этом этапе необходимо выполнить расчеты следующих параметров:

– величина риска;

– критичность реализации каждой угрозы;

– вероятность реализации каждой угрозы через каждую из уязвимостей;

– уровень угрозы по каждой из уязвимостей.

Величина риска (*R*) вычисляется в соответствии с одной из следующих формул:

|  |  |
| --- | --- |
|  | (3.1) |

где Pущ – вероятность ущерба, Cущ – цена ущерба, Pугр – вероятность реализации угрозы, Pуязв – вероятность возникновения уязвимости.

Если информационная система подвержена нескольким (*N*) угрозам, то совокупный Rобщ вычисляется в соответствии со следующей формулой:

|  |  |
| --- | --- |
|  | (3.2) |

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*):

|  |  |
| --- | --- |
|  | (3.3) |

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

|  |  |
| --- | --- |
|  | (3.4) |

5. Управление рисками (Risk management). На этом этапе необходимо предложить меры и средства уменьшения рисков информационной безопасности.

**Практическое задание**

Пусть в результате реализации этапов 1, 2 методики CRAMM было определено, следующее.

1. Количество основных информационных активов организации – 5. Стоимость актива 1 – 1000,00 рублей, актива 2 – 5000,00 рублей, актива 3 – 32000,00 рублей, актива 4 – 100000,00 рублей, актива 5 – 200000,00 рублей.

2. Основными угрозами информационной безопасности организации являются:

– проникновение из сети Интернет в информационную систему организации вредоносного программного обеспечения (угроза 1);

– несанкционированный доступ к информационным активам сотрудника организации (угроза 2).

Вероятность реализации угрозы 1 – 60 %, а угрозы 2 – 40 %.

В результате реализации угрозы 1 наступает последствие «Финансовые потери, связанные с восстановлением ресурсов» (последствие связано с воздействием угрозы 1 на уязвимость 1 информационной системы организации). За прошедший год эта угроза была реализована 5 раз и в результате ее реализации были в полном объеме повреждены активы 1, 2 и 3 и на 30 % был поврежден актив 4. Актив 5 был защищен резервным копированием, в связи с этим его повреждение не повлекло за собой существенных последствий. Кроме того, в результате реализации угрозы 1 наступает последствие «Дезорганизация деятельности компании» (последствие связано с воздействием угрозы 1 на уязвимость 2 информационной системы организации). Цена ущерба, связанного с этим последствием, составляет 20000,00 рублей.

В результате реализации угрозы 2 наступают следующие последствия:

– «Финансовые потери от получения информации конкурентами» (цена ущерба, связанного с этим последствием, составляет 50000,00. руб.);

– «Ущерб репутации организации» (цена ущерба, связанного с этим последствием, составляет 70000,00. руб.).

Первое из указанных последствий связано с воздействием угрозы 2 на уязвимость 1 информационной системы организации, второй – с воздействием угрозы 2 на уязвимость 2 информационной системы организации.

**Задание 1.** Найти цену ущерба по угрозам 1 и 2.

**Задание 2.** Найти величину общего информационного риска.

**Задание 3**. Оценить (в процентах) эффективность мер, принятых для парирования угроз (*E*), если известно, что в результате их использования удалось уменьшить цену ущерба от реализации угрозы 1 в 1,5 раза, а цену ущерба от реализации угрозы 2 – в 2 раза.

**Задание 4**. Установить, чем обусловлены уязвимость 1 и уязвимость 2 информационной системы организации. Предположить подходы по устранению этих уязвимостей (по сути, меры для парирования угроз, воздействующих на эти уязвимости).

**Задание 5.** Найти критичность реализации угрозы 1 через уязвимость 1. Определить для всех выявленных угроз и уязвимостей *Th* и *CTh*, если критичность реализации угрозы 1 через уязвимость 2 составляет 20 %; угрозы 2 через уязвимость 1 – 40 %; угрозы 2 через уязвимость 2 – 30 %.

**Контрольные вопросы**

1. Что такое информационный риск?

2. В чем заключается задача управления информационными рисками?

3. Какие существуют методики оценки рисков и управления ими?

4. Что такое критичность реализации угрозы?

5. Какие этапы включает в себя методика CRAMM оценки информационных рисков?