БГУИР
Кафедра ЗИ

Отчёт
по практическому занятию №3
по теме:
"Анализ рисков информационной безопасности"

Выполнили:
студенты гр. №050502
Крачковский А.В.
Жук Т.С.
Муравицкий М.А.

Проверил:
Столер Д.В.

Минск 2022

Цель: изучить методику анализа рисков информационной безопасности и получить практические навыки по её применению.

Ход работы:

1 Исходные данные для расчёта

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.

1.1 Определение границ исследования

Зададимся структурой корпоративной информационной системы:

Рисунок 1 – Структура корпоративной информационной системы

Пусть в нашем случае информационными активами системы являются:

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

Актив 2. Данные, поступившие за день от разработчиков в СУБД с РМ и удалённо.

Актив 3. Данные, поступившие за день от дизайнеров в СУБД с РМ и удалённо.

Актив 4. Программное обеспечение, используемое в процессе разработки и поддержки и продуктов.

Актив 5. Данные СУБД.

1.2 Стоимость информационных активов

Таблица 1.2 – Стоимость информационных активов в тысячах долларов США

Актив	1	2	3	4	5
Стоимость, К$	0,5	1,0	2,0	2,5	10,0

1.3 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.

1.4 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 3 раза в год и каждый раз повреждало активы:

Актив 1 – на 100%

Актив 2 – на 75%

Актив 3 – на 50%

Актив 4 – на 25%

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 3-кратное в течение года проникновение вредоносного ПО цена ущерба по этому последствию составила $U_{К1/2}$= 2,875 К$ × 3 раза в год.

Таблица 1.4.1 – Ущерб нанесённый реализацией угрозы 1

Актив	1	2	3	4	5
Утрата актива, %	100	75	50	25	0
Последствие 1	+	+	+	+	–
Последствие 2	+	+	+	+	–
Цена ущерба по активу, К$	0,5	0,75	1,0	0,625	0,0

Пусть в результате реализации угрозы 2 наступило первое последствие «Финансовые потери от разглашения и передачи информации конкурентам», причём завербованный конкурентами сотрудник передавал информацию, связанную с активами:

Актив 1 – 25%

Актив 2 – 50%

Актив 3 – 50%

Актив 4 – 25%

Актив 5 – 25%

Сведения об активе 4 находятся в общем доступе либо не представляют значимой коммерческой ценности для конкурентов, поэтому ущербом от утечки этой информации можно пренебречь.

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 $U_{К2/2}$= 4,125 К$ за год.

Таблица 1.4.2 – Ущерб нанесённый реализацией угрозы 2

Актив	1	2	3	4	5
Утечка актива, %	25	50	50	25	25
Последствие 1	+	–	–	–	+
Последствие 2	+	+	+	–	+
Цена ущерба по активу, К$	0,125	0,5	1,0	0,625	2,5

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

1.5 Выбор методов парирования угроз

Пусть методом парирования угрозы 1 является найм специалиста по информационной безопасности, а методом парирования угрозы 2 – разработка и внедрение системы управления доступом к информационным активам.

Заработная плата лучшего специалиста по информационной безопасности: 24 К$ в год (2 К$ в месяц). Стоимость разработки и внедрения наилучшей системы управления доступом к информационным активам – 6 К$ в год.

Утверждённый годовой бюджет на информационную безопасность составляет 20 К$.

2 Расчёты и результаты

2.1 Расчёт цены ущерба по угрозе 1

Рассчитаем цену ущерба по угрозе 1 U_1 по формуле:

$$U_1 = N_1 \cdot (U_{К1/1} + U_{К1/2}) \ ,$$

где N_1 – число реализаций угрозы 1 в год,

$U_{К1/1}$ и $U_{К1/2}$ – ущерб от однократной реализации угрозы 1 по последствиям 1 и 2 соответственно.

$$U_1 = 3 \cdot ((0{,}5 \cdot 1 + 1{,}0 \cdot 0{,}75 + 2{,}0 \cdot 0{,}5 + 2{,}5 \cdot 0{,}25 + 10{,}0 \cdot 0) + 2{,}875) = 3 \cdot (2{,}875 + 2{,}875) = 17{,}25 (К\$)$$

2.2 Расчёт цены ущерба по угрозе 2

Рассчитаем цену ущерба по угрозе 2 U_2 по формуле:

$$U_2 = N_1 \cdot (U_{К2/1} + U_{К2/2}) \ ,$$

где N_2 – число реализаций угрозы 2 в год,

$U_{К2/1}$ и $U_{К2/2}$ – ущерб от однократной реализации угрозы 2 по последствиям 1 и 2 соответственно.

$$U_2 = 1 \cdot ((0{,}5 \cdot 0{,}25 + 1{,}0 \cdot 0 + 2{,}0 \cdot 0 + 2{,}5 \cdot 0 + 10{,}0 \cdot 0{,}25) + 4{,}125) = 2{,}625 + 4{,}125 = 6{,}75 (K\$)$$

2.3 Расчёт общего риска угроз

Рассчитаем общий риск угроз $РИСК_{общий}$ по формуле:

$$РИСК_{общий} = \sum_{i=1}^{N} РИСК_i \ ,$$

где N – число угроз, которым подвержен информационный объект, $РИСК_i$ – риск по i -й угрозе, который, в свою очередь, вычисляется по формуле:

$РИСК_i = p_i \cdot U_i$, где p_i – вероятность ущерба (реализации) i -й угрозы, U_i – цена ущерба (реализации) i -й угрозы.

$$РИСК_1 = p_1 \cdot U_1 = 0{,}6 \cdot 17{,}25 = 10{,}35 (K\$)$$
$$РИСК_2 = p_2 \cdot U_2 = 0{,}4 \cdot 6{,}75 = 2{,}7 (K\$)$$
$$РИСК_{общий} = РИСК_1 + РИСК_2 = 10{,}35 + 2{,}7 = 13{,}05 (K\$)$$

2.4 Определение минимального общего риска угроз после внедрения мер безопасности для парирования угроз

2.4.1 Исходя из критерия «Как, оставаясь в рамках утверждённого 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 заработной платы лучшего специалиста по информационной безопасности позволяет нанять менее квалифицированного специалиста, оставляющего, однако, риск угрозы 2 в размере:

$$РИСК_{ост.1} = РИСК_1 \cdot \frac{x}{100} (K\$)$$

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

$$РИСК_{ост.2} = РИСК_2 \cdot \frac{y}{100} (K\$)$$

Общий риск угроз после внедрения мер должен быть минимально возможным:

$$РИСК_{\text{после внед.мер}} = РИСК_{\text{ост.1}} + РИСК_{\text{ост.2}} \rightarrow min$$

2.4.2 Введём математический аппарат для поиска минимально возможного риска угроз после внедрения мер безопасности

Через переменную t обозначим годовую сумму, которая тратится на систему управления доступом. Пределы её изменения: $t \in [0,6](K\$)$.

Тогда сумма $t' = БЮДЖЕТ - t$, предел изменения которой $t' \in [14,20](K\$)$ будет потрачена на специалиста по информационной безопасности.

Выражаем через переменную t недостатки процентов средств на внедряемые меры безопасности:

$$y(t) = \frac{C_y - t}{C_y} \cdot 100(\%) \quad , \quad x(t) = \frac{C_x - t'}{C_x} \cdot 100 = \frac{C_x - БЮДЖЕТ + t}{C_x} \cdot 100(\%) \quad ,$$

где $C_x = 24\,K\$$ и $C_y = 6\,K\$$ – суммы необходимые для обеспечения полной защищенности посредством каждой отдельно взятой мерой безопасности.

Тогда формула общего риска угроз после внедрения мер примет вид:

$$РИСК_{\text{после внед.мер}}(t) = РИСК_1 \cdot \frac{C_x - БЮДЖЕТ + t}{C_x} + РИСК_2 \cdot \frac{C_y - t}{C_y}$$

После приведения подобных членов получаем:

$$РИСК_{\text{после внед.мер}}(t) = (РИСК_1 + РИСК_2 - РИСК_1 \cdot \frac{БЮДЖЕТ}{C_x}) + (\frac{РИСК_1}{C_x} - \frac{РИСК_2}{C_y}) \cdot t$$

Подставим все константы в полученное выражение:

$$РИСК_{\text{после внед.мер}}(t) = (10{,}35 + 2{,}7 - 10{,}35 \cdot \frac{20}{24}) + (\frac{10{,}35}{24} - \frac{2{,}7}{6}) \cdot t = 21{,}675 - 0{,}01875 \cdot t\,(K\$)$$

Вид функции: линейная. Очевидно, что функция убывающая, т.е. большему значению t соответствует меньшее значение функции $РИСК_{\text{после внед.мер}}(t)$, соответственно при $t = t_{max} \rightarrow РИСК_{\text{после внед.мер}}(t_{max}) = РИСК_{\text{после внед.мер min}}$.

2.4.3 Делаем вывод о наименьшем значении общего риска угроз после внедрения мер при значениях $t = 6\,K\$$, $t' = 14\,K\$$.

$$РИСК_{\text{после внед.мер min}} = 4.3125(K\$)$$

2.5 Оценка эффективности принятых мер безопасности для парирования угроз

Оцениваем эффективность принятых мер безопасности (в процентах) для парирования угроз (EF) по формуле:

$$EF = \frac{РИСК_{ОБЩИЙ} - РИСК_{\text{после внед.мер min}}}{РИСК_{ОБЩИЙ}} = \frac{13{,}05 - 4{,}3125}{13{,}05} = 66{,}954\,\%$$

2.6 Определение критичностей реализаций угроз через уязвимости

2.6.1 Находим критичность реализации угроз через уязвимости как степень влияния однократной реализации угрозы на среднюю работоспособность всех пяти информационных активов системы:

Угрозы 1 через уязвимость 1: $ER_{1/1} = \frac{1+0{,}75+0{,}5+0{,}25+0{,}0}{5} \cdot 100\,\% = 50\,\%$

Угрозы 1 через уязвимость 2: $ER_{1/2} = \frac{1+0{,}75+0{,}5+0{,}25+0{,}0}{5} \cdot 100\,\% = 50\,\%$

Угрозы 2 через уязвимость 1: $ER_{2/1} = \frac{0{,}25+0{,}0+0{,}0+0{,}0+0{,}25}{5} \cdot 100\,\% = 10\,\%$

Угрозы 2 через уязвимость 2: $ER_{2/1} = \frac{0{,}25+0{,}5+0{,}5+0{,}0+0{,}25}{5} \cdot 100\,\% = 30\,\%$

2.6.2 Находим уровни угроз по уязвимостям (вероятности реализации угроз через каждую из уязвимостей ($P(V)$) считаем равными 50 %.):

Угрозы 1 по уязвимости 1: $Th_{1/1} = \frac{ER_{1/1}}{100} \cdot \frac{P(V)}{100} = \frac{50}{100} \cdot \frac{50}{100} = 25\,\%$

Угрозы 1 по уязвимости 2: $Th_{1/2} = \frac{ER_{1/2}}{100} \cdot \frac{P(V)}{100} = \frac{50}{100} \cdot \frac{50}{100} = 25\,\%$

Угрозы 2 по уязвимости 1: $Th_{2/1} = \frac{ER_{2/1}}{100} \cdot \frac{P(V)}{100} = \frac{10}{100} \cdot \frac{50}{100} = 5\,\%$

Угрозы 2 по уязвимости 2: $Th_{2/2} = \frac{ER_{2/2}}{100} \cdot \frac{P(V)}{100} = \frac{30}{100} \cdot \frac{50}{100} = 15\,\%$

2.6.3 Находим уровни угроз по всем уязвимостям:

Угрозы 1 по уязвимостям 1 и 2: $CTh_1 = 1 - \prod_{i=1}^{2} (1 - Th_{1/i}) = 1 - 0{,}75 \cdot 0{,}75 = 0{,}4375$

Угрозы 2 по уязвимостям 1 и 2: $CTh_2 = 1 - \prod_{i=1}^{2} (1 - Th_{2/i}) = 1 - 0{,}95 \cdot 0{,}85 = 0{,}1925$

2.7 Вывод о целесообразности проведения мер противодействия выявленным угрозам и категориях контрмер

Исходя из найденного коэффициента эффективности принятых мер, проведение мер противодействия выгодны так как эффективность больше половины (62.9%).

Категории контрмер:

– обеспечение безопасности инфраструктуры;

– повышения уровня информационной безопасности у персонала.