БГУИР
Кафедра ЗИ

Отчёт
по практическому занятию №3
по теме
“АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ”

Выполнили:
студенты гр. №153502
Бердник Л.А.
Леоненко А.О.
Макаренко А.И.
Сидорова У.Ю.

Проверил:
Столер Д.В.

Минск 2022

Цель работы:

Изучить методику анализа рисков информационной безопасности и получить практические навыки по ее применению.

Этап 1. Определение границ исследований

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.	1000	350	8000	15000	400000

Этап 3. Анализ угроз и уязвимостей

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

Уязвимости: Уязвимости в протоколе VPN. Уязвимости в фаерволе.Уязвимость в соединении с private сектором. Недостаточное требование к защите и сложности паролей.

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

Уязвимости: доступ к ресурсам и данным не соответствующих должности.

Этап 4. Количественные оценки рисков.

Пусть в результате реализации угрозы 1 наступило первое последствие. «Финансовые потери, связанные с восстановлением ресурсов», причем вредоносное ПО проникало в сеть организации 9 раз в год и каждый раз повреждало на 85% активы 1, 3, 4 и на 30% актив 2.

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 9-кратное в течение года проникновение вредоносного ПО цена ущерба по этому последствию составила 3400 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 21700 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 52000 руб. за год.

Вероятность ущерба для угрозы 1 составляет 70%, а для угрозы 2 – 30%.

Этап 5. Выбор методов парирования угроз

Пусть методом парирования угрозы 1 является закупка определенного набора программных средств (фаервола, межсетевого экрана), а методом парирования угрозы 2 – разработка и внедрение системы назначения паролей для доступа к информационным активам.

Стоимость наилучшего фаервола – 12000 руб. Стоимость разработки и внедрения наилучшей системы назначения паролей – 3000 руб. Утверждённый годовой бюджет на информационную безопасность составляет 10000 руб.

Задание 2.1

Найти цену ущерба по угрозе 1:

Ущерб = (0.85*(1000 + 8000 + 15000) +0.3*350)*9 + 3400 = 187945

Задание 2.2

Найти цену ущерба по угрозе 2:

Ущерб = 21700 + 52000 = 73700

Задание 2.3

Найти $РИСК_{общий}$:

$РИСК_{общий}$ = 0.7*187945+0.3*73700 = 153671.5

$$РИСК_{общий} = \sum_{i=1}^{N} p_i * U_i$$

где Ui – $ЦЕНА_{ущерба}$ по i-й угрозе,

pi – $ВЕРОЯТНОСТЬ_{ущерба}$ (весовой коэффициент) i-й угрозы

Задание 2.4

Стоимость наилучшего фаервола – 12000 руб. Стоимость разработки и внедрения наилучшей системы назначения паролей – 3000 руб. Утверждённый годовой бюджет на информационную безопасность составляет 10000 руб.

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

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

$$R_{\text{после внед.мер}} = R_{ост.1} + R_{ост.2}$$

где R_1 – РИСК по 1-й угрозе, руб.,

R_2 – РИСК по 2-й угрозе, руб.

Рассмотрим 4 ситуации:

1) 10000/0:

   R_1= 0.7*187945*(1-10000/12000) = 21926.916

   R_2=0.3*73700*1 = 22110

   $R_{\text{после внед.мер}}$ = 21926.916 + 22110 = 44036.916

2) 9000/1000:

   R_1= 0.7*187945*(1-9000/12000) = 32890.375

   R_2=0.3*73700*(1 - 1/3) = 14740

   $R_{\text{после внед.мер}}$ = 32890.375 + 14740 = 47630.375

3) 8000/2000:

   R_1= 0.7*187945*(1-8/12) = 43853.83

   R_2=0.3*73700*(1 - 2/3) = 7370

   $R_{\text{после внед.мер}}$ = 43853.83 + 7370 = 51223.83

4) 7000/3000

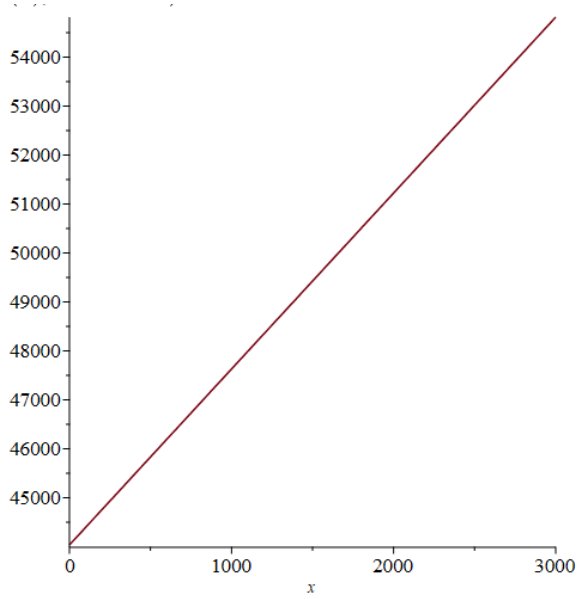
   R_1= 0.7*187945*(1-7/12) = 54817.292

   R_2=0.3*73700*(1 - 1) = 0

   $R_{\text{после внед.мер}}$ = 54817.292 + 0 = 54817.292

Общий риск угроз после внедрения мер должен быть минимально возможным. Таким образом по полученным данным при данных условиях наиболее оптимальным является способ №1 (т.е. 10000 на фаерволл и 0 на разработку и внедрение наилучшей системы назначения паролей).

Также в этом можно убедиться, построив график:



где x - выделенный бюджет на разработку и внедрение системы назначения паролей,

y - общий риск угроз.

Задание 2.5

Эффективность принятых мер безопасности для парирования угроз:

1. EF_1 = 1 - 44036.916/153671.5 = 0.713 или 71%
2. EF_2 = 1 - 47630.375/153671.5 = 0.69 или 69%
3. EF_3 = 1 - 51223.83/153671.5 = 0.667 или 67%
4. EF_4 = 1 - 54817.292/153671.5 = 0.643 или 64%

Таким образом риск угроз уменьшится на наибольший процент(71%) по сравнению с начальным общим риском при 1 случае.

Задание 2.6

$$Th = \frac{ER}{100} * \frac{P(V)}{100}$$

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

Критичность реализации угрозы 1 через уязвимость 1 (ER1/1):

$ER_{1/1} = (85 + 30 + 85 + 85 + 0)/5 = 57\%$

– уровень угрозы 1 по уязвимости 1 (Th1/1):

$$Th_{1/1} = \frac{57}{100} * \frac{50}{100} = 0.285 \text{ или } 29\%$$

– уровень угрозы 1 по уязвимости 2 (Th1/2):

$$Th_{1/2} = \frac{20}{100} * \frac{50}{100} = 0.1 \text{ или } 10\%$$

– уровень угрозы 2 по уязвимости 1 (Th2/1):

$$Th_{2/1} = \frac{30}{100} * \frac{50}{100} = 0.15 \text{ или } 15\%$$

– уровень угрозы 2 по уязвимости 2 (Th2/2):

$$Th_{2/2} = \frac{40}{100} * \frac{50}{100} = 0.20 \text{ или } 20\%$$

– уровень угрозы 1 по всем (двум) уязвимостям (CTh1):

$CTh_1 = 1 - (1 - 0.285)*(1 - 0.1) = 0.357$ или 36%

– уровень угрозы 2 по всем (двум) уязвимостям (CTh2):

$CTh_2 = 1 - (1 - 0.15)*(1 - 0.2) = 0.32$ или 32%

Задание 2.7

Вывод

В результате нашей работы были проанализированы риски в части информационных активов с помощью методики CRAMM, а также предложены некоторые средства контроля и управления рисками, адекватные целям и задачам бизнеса компании.

Была проведена количественная оценка рисков: найдены цены ущерба по данным угрозам, вероятности ущерба для угроз, критичности реализации угроз через уязвимость, рассмотрены реализации угроз и их последствия, проанализирована эффективность принятых мер безопасности для парирования угроз.

Также на основании полученных результатов был сделан вывод об общем риске угроз после внедрения мер и изменении риска угроз по сравнению с начальным общим риском.

По полученным результатам общая целесообразность проведения мер противодействия выявленным угрозам оказалась обоснованной. При правильном распределении бюджета организации, эффективность принятых мер безопасности для парирования угроз составит 71%.