БГУИР
Кафедра ЗИ

Отчёт
по практическому занятию №2
по теме: «Анализ рисков информационной безопасности»

Выполнили
студенты группы 950501:
Деркач А.В.
Романчук А.В.

Проверил:
Столер Д.В

Минск 2021

1. Исходные данные для выполнения

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 информацию.

2. Выполнение практического задания

Задание 2.1. Найти цену ущерба по угрозе 1.

$$U_1 = (700 + 500 + 3200) \cdot 6 + 0,2 \cdot 9000 \cdot 6 + 2100 = 26400 + 10800 + 2100 = 39300\ (руб.)$$

Данные для расчета были взяты из этапа 2 и 4.

Задание 2.2. Найти цену ущерба по угрозе 2.

$$U_2 = 17600 + 33000 = 50600\ (руб.)$$

Данные для расчета были взяты из этапа 2 и 4.

Задание 2.3. Найти $\text{РИСК}_{\text{общий}}$.

$$\text{РИСК}_{общий} = \sum_{i=1}^{N} p_i \cdot U_i = 0,6 \cdot 39300 + 0,4 \cdot 50600 = 43820\ (руб.)$$

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

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

$$\sum_{i=1}^{N} p_i = 1$$

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.

Рассчитаем РИСК по 1-й угрозе:

$$R_1 = p_1 \cdot U_1 = 0,6 \cdot 39300 = 23580\ (руб.)$$

Рассчитаем РИСК по 2-й угрозе:

$$R_2 = p_2 \cdot U_2 = 0,4 \cdot 50600 = 20240\ (руб.)$$

Далее мы рассмотрим 3 способа распределения средств бюджета (8000 руб.). Для этого мы будем пользоваться следующими формулами:

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

$$R_{ост.1} = R_1 \cdot \frac{x}{100}$$

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:

$$R_{ост.2} = R_2 \cdot \frac{y}{100}$$

где R2 – РИСК по 2-й угрозе, руб.;

Общий риск угроз после внедрения мер должен быть минимально возможным:

$$R_{после\_внед.мер} = (R_{ост.1} + R_{ост.2}) \to \min$$

Рассмотрим 1-й способ (8000 руб. на фаерволл, тогда на систему назначения паролей остается – 0 руб.):

$$x_1 = \frac{9000 - 8000}{9000} \cdot 100\% \approx 11\%$$

$$y_1 = \frac{2000 - 0}{2000} \cdot 100\% = 100\%$$

$$R_{ост.1} = R_1 \cdot \frac{x_1}{100} = 23580 \cdot \frac{11}{100} = 2593{,}80\ (руб.)$$

$$R_{ост.2} = R_2 \cdot \frac{y_1}{100} = 20240 \cdot \frac{100}{100} = 20240\ (руб.)$$

$$R_{после\_внед.мер.1} = R_{ост.1} + R_{ост.2} = 22833{,}80\ (руб.)$$

Рассмотрим 2-й способ (7000 руб. на фаерволл, тогда на систему назначения паролей остается – 1000 руб.):

$$x_2 = \frac{9000 - 7000}{9000} \cdot 100\% \approx 22\%$$

$$y_2 = \frac{2000 - 1000}{2000} \cdot 100\% = 50\%$$

$$R_{ост.1} = R_1 \cdot \frac{x_2}{100} = 23580 \cdot \frac{22}{100} = 5187{,}60\ (руб.)$$

$$R_{ост.2} = R_2 \cdot \frac{y_2}{100} = 20240 \cdot \frac{50}{100} = 10120\ (руб.)$$

$$R_{после\_внед.мер.2} = R_{ост.1} + R_{ост.2} = 15307{,}60\ (руб.)$$

Рассмотрим 3-й способ (6000 руб. на фаерволл, тогда на систему назначения паролей остается – 2000 руб.):

$$x_3 = \frac{9000 - 6000}{9000} \cdot 100\% \approx 33\%$$

$$y_3 = \frac{2000 - 2000}{2000} \cdot 100\% = 0\%$$

$$R_{ост.1} = R_1 \cdot \frac{x_3}{100} = 23580 \cdot \frac{33}{100} = 7781{,}4\ (руб.)$$

$$R_{ост.2} = R_2 \cdot \frac{y_3}{100} = 20240 \cdot \frac{0}{100} = 0\ (руб.)$$

$$R_{после\_внед.мер.3} = R_{ост.1} + R_{ост.2} = 7781{,}4\ (руб.)$$

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.

$$EF_1 = \frac{РИСК_{общий} - R_{после\_внед.мер.1}}{РИСК_{общий}} \cdot 100\% = \frac{43820 - 22833,8}{43820} \cdot 100\% = 47,9\%$$

$$EF_2 = \frac{РИСК_{общий} - R_{после\_внед.мер.2}}{РИСК_{общий}} \cdot 100\% = \frac{43820 - 15307,60}{43820} \cdot 100\% = 65,1\%$$

$$EF_3 = \frac{РИСК_{общий} - R_{после\_внед.мер.3}}{РИСК_{общий}} \cdot 100\% = \frac{43820 - 7781,4}{43820} \cdot 100\% = 82,2\%$$

Наиболее эффективным является $EF_3 = 82,2\%$

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 (Th1/1);
– уровень угрозы 1 по уязвимости 2 (Th1/2);
– уровень угрозы 2 по уязвимости 1 (Th2/1);
– уровень угрозы 2 по уязвимости 2 (Th2/2);
– уровень угрозы 1 по всем (двум) уязвимостям (CTh1);
– уровень угрозы 2 по всем (двум) уязвимостям (CTh2).

Для расчета будем использовать следующие формулы:

Уровень угрозы по уязвимости (Th):

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

где ER (критичность реализации угрозы) — степень влияния реализации угрозы на ресурс, т.е. как сильно повлияет угроза на работу ресурса;

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

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

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

Найдем критичность реализации угрозы 1 через уязвимость 1 ($ER_{1/1}$):

$$ER_{1/1} = \frac{100 \cdot (1+1+1+0,2+0)}{5} \cdot 100\% = \frac{320}{5} \cdot 100\% = 64\%$$

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 %. Произведем расчеты:

Уровень угрозы 1 по уязвимости 1 ($Th_{1/1}$):

$$Th_{1/1} = \frac{ER_{1/1}}{100} \cdot \frac{P(V)}{100} = \frac{64}{100} \cdot \frac{50}{100} \cdot 100\% = 32\%$$

Уровень угрозы 1 по уязвимости 2 ($Th_{1/2}$):

$$Th_{1/2} = \frac{ER_{1/2}}{100} \cdot \frac{P(V)}{100} = \frac{20}{100} \cdot \frac{50}{100} \cdot 100\% = 10\%$$

Уровень угрозы 2 по уязвимости 1 ($Th_{2/1}$):

$$Th_{2/1} = \frac{ER_{2/1}}{100} \cdot \frac{P(V)}{100} = \frac{30}{100} \cdot \frac{50}{100} \cdot 100\% = 15\%$$

Уровень угрозы 2 по уязвимости 2 ($Th_{2/2}$):

$$Th_{2/2} = \frac{ER_{2/2}}{100} \cdot \frac{P(V)}{100} = \frac{40}{100} \cdot \frac{50}{100} \cdot 100\% = 20\%$$

Уровень угрозы 1 по двум уязвимостям (CTh_1):

$$CTh_1 = 1 - \prod_{i=1}^{2} (1 - Th_i) = 1 - 0,68 \cdot 0,9 = 1 - 0,612 = 0,39$$

Уровень угрозы 2 по двум уязвимостям (CTh_2):

$$CTh_2 = 1 - \prod_{i=1}^{2}(1 - Th_i) = 1 - 0,85 \cdot 0,80 = 0,32$$

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

Исходя из полученных расчетов, проведение мер противодействия выявленным угрозам целесообразно т.к. эффективность принятых мер безопасности 82%, что является довольно высоким показателем.

Категории контрмер, к которым можно отнести предлагаемые методы парирования, следующие:

- обеспечение безопасности на сетевом уровне;
- обеспечение безопасности поддерживающей инфраструктуры.