БГУИР

Кафедра ЗИ

Отчет

по практическому занятию №5

по теме:

«АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выполнили: Проверил:

Студенты гр.150503 Столер Д.В.

Ходосевич М.А.  
Семков А.Д.  
Шарай П.Ю.  
Гайчук В.Н.

Минск 2023

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

*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.

Уязвимость 1.1. Отсутствие антивирусного ПО.

Уязвимость 1.2. Устаревшее программное обеспечение.

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

Уязвимость 2.1. Отсутствие ограничения доступа к информационным активам компании.

Уязвимость 2.2. Отсутствие мониторинга действий сотрудника на персональном компьютере в компании.

*Этап 4. Количественные оценки рисков.*

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

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.

ЦЕНАущерба1 = 6\*(100%\*(700+500+3200)+20%\*9000)+2100=39300 (руб.)

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

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.

ЦЕНАущерба2 = 17600 + 33000 = 50600 (руб.)

***Задание 2.3.*** Найти РИСКобщий.

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

РИСКугрозы1= ЦЕНАущерба1\*ВЕРОЯТНОСТЬугрозы1=23580 (руб.)

РИСКугрозы2= ЦЕНАущерба2\*ВЕРОЯТНОСТЬугрозы2=20240 (руб.)

РИСКобщий= РИСКугрозы1+ РИСКугрозы2=23580=43820 (руб.)

*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 2.4.***

Рассмотрим 3 способа распределения выделенных средств бюджета:

1. На файрвол выделяется 8000 руб., на систему назначения паролей – 0 руб.
2. На файрвол выделяется 7000 руб., на систему назначения паролей – 1000 руб.
3. На файрвол выделяется 6000 руб., на систему назначения паролей – 2000 руб.

***Задание 2.5.***

Оценим эффективность принятых мер безопасности для каждого способа распределения выделенных средств:

***Задание 2.6.***

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 %:

Вычислим критичность реализации угрозы 1 через уязвимость 1:

Вычислим уровни угроз по уязвимостям:

Вычислим уровни угроз по всем реализующимся уязвимостям

Этап 6. Вывод

***Задание 2.7.***

Вывод о целесообразности проведения мер противодействия выявленным угрозам:

Было рассмотрено 3 способа закупки программных средств за выделенный годовой бюджет на информационную безопасность. Самым эффективным оказался вариант разработки и внедрения наилучшей системы назначения паролей с последующим выделением остаточных средств на закупку наилучшего файрвола. Данный способ оказался самым эффективным, так как для разработки и внедрения наилучшей СНП требуется значительно меньшее количество средств (2000 руб.), чем для закупки наилучшего файрвола (9000 руб.), а уровень риска у каждой угрозы примерно одинаков (23580 руб. и 20240 руб. соответственно).

Предлагаемые методы парирования угроз можно отнести к следующим контрмерам:

1. Обеспечение безопасности на сетевом уровне.
2. Обеспечение безопасности на уровне системного администратора.