БГУИР

Кафедра ЭВМ

Отчет по практическому занятию № 5

Тема: «Анализ рисков информационной безопасности»

Выполнили:

студенты гр. №150502

Альхимович Н.Г.

Катковская Е.А.

Скалозуб К.А.

Сацюк Я.И.

Проверил:

Столер Д.В.

Минск

2023

Цель: 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: фишинговые рассылки по электронной почте.

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

Уязвимость 2.1: отсутствие пропускной системы.

Уязвимость 2.2: отсутствие парольной защиты на ПК.

*Этап 4. Количественные оценки рисков.*

Задание 2.1

Цена ущерба по 1-ой угрозе = ((700+500+3200) \* 1 + 9000\*0,2) \* 6 + 2.100 = 39.300 (руб.)

Задание 2.2

Цена ущерба по 2-ой угрозе = 17.600 + 33.000 = 50.600 (руб.)

Задание 2.3

Рискобщий = вероятность ущерба по 1-ой угрозе \* цена ущерба по 1-ой угрозе + вероятность ущерба по 2-ой угрозе \* цена ущерба по 2-ой угрозе = 39.300 \* 0,6 + 50.600 \* 0,4 = 23.580 + 20.240 = 43.820 (руб.)

*Этап 5. Выбор методов парирования угроз.*

Задание 2.4

R1 = 23.580 руб.

R2 = 20.240 руб.

Можно выделить 3 способа распределения выделенных средств на парирование угроз 1 и 2:

1. на файрволл– 8000 руб., тогда на систему назначения паролей остается – 0 руб.

x = (9000-8000) / 9000 = 11%

y = (2000-0) / 2000 = 100%

Rост.1 = R1 \* x / 100 = 2.594 (руб.)

Rост.2 = R2 \* y / 100 = 20.240 (руб.)

Rпосле внедр. мер = (Rост.1 + Rост.2 ) = 22.834 (руб.)

1. на файрволл – 7000 руб., тогда на систему назначения паролей остается – 1000 руб.

x = (9000-7000) / 9000 = 22%

y = (2000-1000) / 2000 = 50%

Rост.1 = R1 \* x / 100 = 5.188 (руб.)

Rост.2 = R2 \* y / 100 = 10.120 (руб.)

Rпосле внедр. мер = (Rост.1 + Rост.2 ) = 15.308 (руб.)

1. на систему назначения паролей – 2000 руб., тогда на файрволл – 6000 руб.

x = (9000-6000) / 9000 = 33%

y = (2000-2000) / 2000 = 0%

Rост.1 = R1 \* x / 100 = 7.781 (руб.)

Rост.2 = R2 \* y / 100 = 0 (руб.)

Rпосле внедр. мер = (Rост.1 + Rост.2 ) = 7.781 (руб.)

В результате, минимальный общий риск угроз возможен при третьем случае (на систему назначения паролей – 2000 руб., тогда на файрволл– 6000 руб.).

Задание 2.5

EF = (Rобщий - Rпосле внедр. мер) / Rобщий = (43.820 – 7.781) / 43.820 \* 100% = 36.039 / 43.820 \* 100%= 0,82 \* 100% = 82%

Задание 2.6

ER1/1 = (100% + 100% + 100% + 20% + 0%) / 5 = 64%

Th1/1 = ER1/1/100 \* P(V)/100 = 64%/100% \* 50%/100% = 0,32

Th1/2 = ER1/2/100 \* P(V)/100 = 20%/100% \* 50%/100% = 0,1

Th2/1 = ER2/1/100 \* P(V)/100 = 30%/100% \* 50%/100% = 0,15

Th2/2 = ER2/2/100 \* P(V)/100 = 40%/100% \* 50%/100% = 0,2

CTh1 = = 1 – (1-Th1/1)\*(1-Th1/2) = 1 – (1-0,32)\*(1-0,1) = 1 – 0,68\*0,9 = 1 – 0,612 = 0,388

CTh2 = = 1 – (1-Th2/1)\*(1-Th2/2) = 1 – 0,85\*0,8 = 1 – 0,68 = 0,32

Вывод: предложенные методы парирования угроз целесообразны в случае, если применяется третий вариант распределения средств годового бюджета: на систему назначения паролей – 2000 руб., тогда на файрволл – 6000 руб. Эффективность принятых мер в таком случае составляет 82%.

Метод парирования угрозы 1 в виде файрволла относится к группе контрмер – обеспечение безопасности на сетевом уровне, а метод парирования угрозы 2 в виде системы назначения паролей для доступа к информационным активам относится к группе контрмер – обеспечение безопасности на уровне системного администратора.