Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

Кафедра защиты информации

ОТЧЕТ

Практическое занятие №5

«Анализ рисков информационной безопасности»

Выполнили:

студенты гр. № 251003

Кухоцковолец А. М.

Габрусь С. П.

Панкратьев Е. С

Проверил:

Столер Д.В.

Минск 2024

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

Результаты выполнения практического задания.

*Этап 1. Определение границ исследования.*

Для этого определяется состав и структура основных информационных активов системы. Пусть в данном 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: Устаревшее программное обеспечение (браузеры и антивирусные программы)

Уязвимость 1.2: Недостаточная обученность персонала (несоблюдение сотрудниками правил безопасности, таких как открытие вредоносных вложений в электронных письмах или переход по подозрительным ссылкам.)

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

Уязвимость 2.1: Недостаточная защита конфиденциальной информации. (неэффективное управление правами доступа, что позволяет сотрудникам иметь больше прав, чем им не следует)

Уязвимость 2.2: Недостаточный мониторинг и аудит действий пользователей. (отсутствие системы мониторинга действий пользователей, что делает невозможным обнаружение подозрительной активности, такой как необычный объем скачиваемых данных или попытки несанкционированного доступа.)

*Этап 4. Количественные оценки рисков.*

Результаты расчета по заданиям 2.1-2.3, а именно:

Цена ущерба по угрозе 1:

Ц1 = (700 + 500 + 3200 + (0.2 \* 9000)) \* 6 (раз в год) + 2100 = 39 300 р/год

Цена ущерба по угрозе 2:

Ц2 = 17 600 + 33 000 = 50 600 р/год

Общий риск:

Rобщий = 0.6 \* 39 300 + 0.4 \* 50 600 = 43 820 р

*Этап 5. Выбор методов парирования угроз.*

Результаты расчета по заданиям 2.4-2.6, а именно:

Рассмотрим 3 способа распределения средств бюджета (8000 руб.) на парирование угроз №1-2:

1) на фаерволл – 8000 руб., тогда на систему назначения паролей остается – 0 руб.;

2) на фаерволл – 7000 руб., тогда на систему назначения паролей – 1000 руб.;

3) на фаерволл – 6000 руб., тогда на систему назначения паролей – 2000 руб.

1) Rост.1 = 11% \* 23580 = 2593.8 р

Rост.2 = 100% \* 20240 = 20240 р

2) Rост.1 = 22% \* 23580 = 5187.6 р

Rост.2 = 50% \* 20240 = 10120 р

3) Rост.1 = 33% \* 23580 = 7781.4 р

Rост.2 = 0% \* 20240 = 0

Оптимальным вариантом распределения средств бюджета является способ №3.

Эффективность принятых мер безопасности для парирования угроз для оптимального варианта распределения средств бюджета составила:

*EF* = 100% - (7781.4 / 43820) \* 100% = 82.24%

Критичность реализации угрозы 1 через уязвимость 1:

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

Уровень угрозы 1 по уязвимости 1:

*Th1/1* = (64 / 100) \* (50 / 100) = 0.32

Уровень угрозы 1 по уязвимости 2:

*Th1/2* = (20 / 100) \* (50 / 100) = 0.1

Уровень угрозы 2 по уязвимости 1:

*Th2/1* = (30 / 100) \* (50 / 100) = 0.15

Уровень угрозы 2 по уязвимости 2:

*Th2/2* = (40 / 100) \* (50 / 100) = 0.2

Уровень угрозы 1 по двум уязвимостям:

*CTh1* = 1 – ((1 – 0.32) \* (1 – 0.1)) = 0.388

Уровень угрозы 2 по двум уязвимостям:

*CTh2* = 1 – ((1 - 0.15) \* (1 – 0.2)) = 0.32

*Этап 6. Выводы.*

Задание 2.7. Целесообразно проводить мероприятия по противодействию мер, так как риск уменьшился на 82.24%. Защита межсетевого экрана (фаервола) относится к контрмере обеспечение безопасности на сетевом уровне, разработка и внедрение наилучшей системы назначения паролей – обеспечению безопасности на уровне системного администратора.