Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра ЗИ

Отчет

Практическое занятие №5

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнили студент гр. 150504: Проверил:

Горбачевский М.В. Столер Д.В.

Горбачевский К.В.

Донцу В.С.

Желубовский С.В .

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 | 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 2: Отсутствие антивирусного ПО

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

- Уязвимость 2: Отсутствие разграничения прав сотрудников, в зависимости от занимаемой должности.

**Этап 4.** Количественные оценки рисков.

Угроза 1: (Последствия 1 и 2)

РИСК\_1 = 6 \* 0.6 \* (700 + 500 + 3200 + 0.2\*9000) + 0.6\*2100 = 23580

Угроза 2: (Последствия 1 и 2)

РИСК\_2 = 0.4\*(17600 + 33000) = 20240

РИСК\_О = 20240 + 23580 = 43820

**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 2.1.**

Цена ущерба от угрозы 1: 23580

**Задание 2.2.**

Цена ущерба от угрозы 2: 20240

**Задание 2.3.**

Цена ущерба(общая): 43820

**Задание 2.3.**

Рассмотрим три случая распределения бюджета(общий риск угроз после внедрения мер должен быть минимально возможным)

1. 7500руб на фаерволл и 1500руб на систему паролей
2. 7000руб на фаерволл и 1000руб на систему паролей
3. 6000руб на фаерволл и 2000руб на систему паролей
4. 7300руб на фаерволл и 1700руб на систему паролей

Рассчитаем остаточные риски:

1. R после внед.мер = R1 + R2 = 16%\*РИСК\_1 + 25%\*РИСК\_2 = 3772 + 5060 = 8832
2. R после внед.мер = R1 + R2 = 22%\*РИСК\_1 + 50%\*РИСК\_2 = 5187 + 10120 = 15307
3. R после внед.мер = R1 + R2 = 33%\*РИСК\_1 + 0%\*РИСК\_2 = 7781 + 20240 = 28021
4. R после внед.мер = R1 + R2 = 19%\*РИСК\_1 + 15%\*РИСК\_2 = 4480 + 3036 = 7516

**Задание 2.5.**

Риск после внедрения методов парирования уменьшится по сравнению с первоначальным на 100% - 7516/43820 = 87% или на 36304руб в денежном эквиваленте.

**Задание 2.6.**

Критичность реализации угрозы 1 от уязвимости 1: (100% + 100% + 100% + 20% + 0%) / 5 = 64%

**Задание 2.7.**

Внедрение мер является целесообразным так как риски при реализации угрозы значительно уменьшаются (на 87%).

Предлагаемые методы парирования угроз можно отнести к следующим типам контрмер:

1. обеспечение безопасности на сетевом уровне;
2. обеспечение безопасности на уровне системного администратора.