Министерство образования Республики Беларусь Учреждение образования Белорусский государственный университет информатики и радиоэлектроники

Кафедра защиты информации

Основы информационной безопасности

Отчет

по практическому занятию 5

по теме

“АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ”

Выполнили: Проверил

Студенты группы 150504 Столер Д.В.

Бобылёв Н.С.

Нестеренко А.Э.

Минск 2023

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

Проанализируем риски только в части информационных активов с помощью методики CRAMM и предложим некоторые средства контроля и управления рисками, адекватные целям и задачам бизнеса компании.

**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 СУБцД 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.

Стоимость активов 1 2 3 4 5 соответственно 700 500 3200 9000 500000 руб.

**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 им информацию.

**Этап 4**. Количественные оценки рисков

Цена ущерба 1 угрозы: 6(700+500+3200+20%9000)+2100=39300руб

Цена ущерба 2 угрозы:17600+33000=50600 руб

Риск общий=60%39300+40%50600=43820 руб

**Этап 5**. Выбор методов парирования угроз.

5.1 7000 руб на фаервол и 1000 руб на СНП;

Х=(9000-7000)/9000= 22% y=(2000-1000)/2000=50%

Ro1=22320\*22/100=4910 руб

Ro2=20240\*50/100=10120 руб

Rпосле=4910+10120=15030 руб

5.2 7500 руб на фаервол и 500 руб на СНП;

Х=(9000-7500)/9000= 17% y=(2000-500)/2000=25%

Ro1=22320\*17/100=3794 руб

Ro2=20240\*25/100=5060 руб

Rпосле=8854 руб

5.3 8000 руб на фаервол и 0 руб на СНП;

Х=(9000-8000)/9000= 11% y=(2000-0)/2000=100%

Ro1=22320\*11/100=2455 руб

Ro2=20240\*100/100=20240 руб

Rпосле=22695 руб

При распределении бюджета 7500 руб на первую угрозу и 500 руб на вторую риск минимален из возможных проверенных вариантов.

Эффективность принятых мер безопасности (в процентах) для парирования угроз:

EF =(42560-8854)/42560=79%

Критичность реализации угрозы:

ER1/1 = (100\*3+20)/5=64%;

Th 1/1= 064\*0,5=0,32;

Th1/2 = 0,2\*0,5=0,1;

Th2/1 = 0,3\*0,5=0,15;

Th2/2 = 0,4\*0,5=0,2;

CTh1 = 1-((1-0,32)\*(1-0,1))=38,8%;

CTh2 = 1-((1-0,15)\*(1-0,2))=32%;

**Вывод**

Проведение мер безопасности были целесообразны так как риски уменьшились на 79%

Категории контрмер, к которым можно отнести предлагаемые методы парирования из пятого этапа: – обеспечение безопасности на сетевом уровне; – обеспечение безопасности на уровне системного администратора.