Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ЗИ

Практическое задание №3

Выполнил: Суворов И.С.

гр.962991

Проверила: Саванович С.Э.

Минск 2021

Пусть в результате реализации этапов 1, 2 методики CRAMM было определено, следующее.

1. Количество основных информационных активов организации – 5. Стоимость актива 1 – 1000,00 рублей, актива 2 – 5000,00 рублей, актива 3 – 32000,00 рублей, актива 4 – 100000,00 рублей, актива 5 – 200000,00 рублей.

2. Основными угрозами информационной безопасности организации являются:

– проникновение из сети Интернет в информационную систему организации вредоносного программного обеспечения (угроза 1);

– несанкционированный доступ к информационным активам сотрудника организации (угроза 2).

Вероятность реализации угрозы 1 – 60 %, а угрозы 2 – 40 %.

В результате реализации угрозы 1 наступает последствие «Финансовые потери, связанные с восстановлением ресурсов» (последствие связано с воздействием угрозы 1 на уязвимость 1 информационной системы организации). За прошедший год эта угроза была реализована 5 раз и в результате ее реализации были в полном объеме повреждены активы 1, 2 и 3 и на 30 % был поврежден актив 4. Актив 5 был защищен резервным копированием, в связи с этим его повреждение не повлекло за собой существенных последствий. Кроме того, в результате реализации угрозы 1 наступает последствие «Дезорганизация деятельности компании» (последствие связано с воздействием угрозы 1 на уязвимость 2 информационной системы организации). Цена ущерба, связанного с этим последствием, составляет 20000,00 рублей.

В результате реализации угрозы 2 наступают следующие последствия:

– «Финансовые потери от получения информации конкурентами» (цена ущерба, связанного с этим последствием, составляет 50000,00. руб.);

– «Ущерб репутации организации» (цена ущерба, связанного с этим последствием, составляет 70000,00. руб.).

Первое из указанных последствий связано с воздействием угрозы 2 на уязвимость 1 информационной системы организации, второй – с воздействием угрозы 2 на уязвимость 2 информационной системы организации.

**Задание 2.3.1.1** Найти цену ущерба по угрозам 1 и 2.

**Задание 2.3.1.2** Определить величину общего информационного риска.

**Задание 2.3.1.3** Оценить (в процентах) эффективность мер, принятых для парирования угроз (*E*), если известно, что в результате их использования удалось уменьшить цену ущерба от реализации угрозы 1 в 1,5 раза, а цену ущерба от реализации угрозы 2 – в 2 раза.

**Задание 2.3.1.4**Найти критичность реализации угрозы 1 через уязвимость 1. Определить для всех выявленных угроз и уязвимостей *Th* и *CTh*, если критичность реализации угрозы 1 через уязвимость 2 составляет 20 %; угрозы 2 через уязвимость 1 – 40 %; угрозы 2 через уязвимость 2 – 30 %.

**Задание 2.3.1.5** Установить, чем обусловлены уязвимость 1 и уязвимость 2 информационной системы организации. Предложить подходы по устранению этих уязвимостей (по сути, меры для парирования угроз, воздействующих на эти уязвимости).

1. С1ущ = 5\*(1000+5000+32000+30000) + 20000 = 365 тыс.

С2ущ = 70000 + 50000 = 120 тыс.

1. Rобщ = 0.6\*360000 + 0.4\*120000 = 216000 + 48000 = 264 тыс.
2. E = (R1ппм – R2ппм)/Rобщ.ппм \* 100% = (264 – 168)/61 \* 100% = 36,4 %
3. ER1/1 = 330%/5 = 66%

Th1/1 = 66/100 \* 50/100 = 0.33

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

Th2/1 = 40/100 \* 50/100 = 0.2

Th2/2 = 30/100 \* 50/100 = 0.15

CTh1 = 1 – (1 – Th1/1) \* (1 – Th1/2) = 1 – (1 – 0.33) \* (1 – 0.1) = 0.397

CTh2 = 1 – (1 – Th2/1) \* (1 – Th2/2) = 1 – (1 – 0.2) \* (1 – 0.15) = 0.32

Вывод: Для того чтобы снизить риск информационной безопасности необходимо предложить подходы для устранения этих уязвимостей (меры для ликвидации угроз воздействующих на эти уязвимости).