БГУИР

Кафедра ЗИ

Отчёт

По практическому занятию №3

По теме

«АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выполнили:
Студенты гр.№153501
Тимофеев К.А.
Глебцова Е.Н.
Шевцова Д.С.

Проверил:
Столер Д.В.

Минск 2022

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

Этапы

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

Задание 2.1. Найти цену ущерба по угрозе проникновения из Интернета в сеть организации вредоносного программного обеспечения.

C_1=100%*(700+500+3200)*6+20%*9000*6+0*500000+2100=39300 (р)

Задание 2.2. Найти цену ущерба при несанкционированном доступе к информационным активам сотрудника
компании, завербованного конкурентами и передающего им информацию.

C_2= 17600 + 33000 = 50600 (р)

Задание 2.3. Найти $Риск_{общий}$

$R_1 = C_1 * 0.6 = 23580$ (р)
$R_2 = C_2 * 0.4 = 20240$ (р)
$R_{общий} = R_1 + R_2 = 43820$ (р)

Задание 2.4.

n	X_n, р	Y_n, р	$R_{p.n}$, р

1	8000	0	22860
2	7000	1000	15360
3	6000	2000	7860

$R_{p.1} = R_1 * (9000 – X_1)/9000 + R_2*(8000 – Y)/2000 = 22860$ (р)
$R_{p.2} = 15360$ (р)
$R_{p.3} = 7860$ (р)

Задание 2.5. Оценить эффективность принятых мер безопасности (в процентах) для парирования угроз (EF), т.е. на сколько процентов уменьшится риск до внедрения мер (риск общий) по сравнению с минимальным риском после их внедрения.

n	X_n, р	Y_n, р	$R_{p.n}$, р	E_n, %
1	8000	0	22860	47.8
2	7000	1000	15360	65
3	6000	2000	7860	82

$E_1 = (R_{общ} - R_{p.1}) / R_{общ} = 0.478 = 47.8$ %
$E_2 = 0.65 = 65$ %
$E_3 = 0.82 = 82$ %

Задание 2.6.

$ER_{1/1} = (100\% + 100\% + 100\% + 20\% + 0\%) / 5 = 64\%$
$ER_{1/2} = 20\%$
$ER_{2/1} = 30\%$
$ER_{2/2} = 40\%$
$P(V) = 50\%$

$Th_{1/1} = (ER_{1/1} / 100) * (P(V) / 100) = 0.32$
$Th_{1/2} = 0.1$
$Th_{2/1} = 0.15$
$Th_{2/2} = 0.2$
$CTh_1 = 1- \Pi_{i=1..n} (1 – Th_n) = 1- (1 – Th_{1/1})*(1 – Th_{1/2}) = 0.39$
$Cth_2 = 0.32$

2.7. Вывод
По полученным эффективностям принятых мер безопасности можно сделать вывод, что самым эффективным разделением бюджета будет третий, а именно 2000 на лучшую систему назначения паролей и 6000 на фаерволл(эффективность достигает 82%). Используемые контрмеры относятся к категориям обеспечения безопасности на сетевом уровне и обеспечения физической безопасности.