БГУИР

Кафедра ЗИ

Отчёт

по практическому занятию №3

по теме: «Анализ рисков информационной безопасности»

Выполнили Проверил:

студенты группы 030501: Столер Д.В.

Вайтехович П.В.

Потапов С.А.

Приёмко Д.С.

Присяжнюк Н.А.

Минск 2022

1. **Цель работы**

Изучить методику анализа рисков информационной безопасности и получить практические навыки по ее применению.

1. **Выполнение практического задания**

***Задание 2.1.*** Найти цену ущерба по угрозе 1.

Угроза 1 – проникновение из Интернета в сеть организации вредоносного ПО.

***Задание 2.2.*** Найти цену ущерба по угрозе 2.

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

***Задание 2.3.*** Найти

***Задание 2.4.*** Исходя из критерия “Как, оставаясь в рамках утвержденного годового бюджета на информационную безопасность достигнуть максимального уровня защищенности информационных активов компании (минимум риска)?” требуется оптимально распределить средства годового бюджета (8000 руб.) на парирование угрозы 1 и парирование угрозы 2, считая, что для рассматриваемой корпоративной информационной системы экспертным путём установлено, что:

* недостаток каждых *х* % средств от стоимости наилучшего фаерволла позволяет приобрести более дешёвый фаерволл, оставляющий, однако, риск угрозы 1 в размере:

(7)

где *R1* – РИСК по 1-й угрозе, руб.;

* недостаток каждых *у* % средств от стоимости наилучшей системы назначения паролей позволяет приобрести более дешёвую систему, оставляющую, однако, риск угрозы 2 в размере:

(8)

где *R2* – РИСК по 2-й угрозе, руб.;

Общий риск угроз после внедрения мер должен быть минимально возможным:

*Rпосле внед.мер* = (*Rост*.*1* + *Rост*.*2* ) → *min* (9)

Можно выделить *N* способов распределения выделенных средств на парирование угроз 1 и 2, например, случай 1: на фаерволл – 8000 руб., тогда на систему назначения паролей остается – 0 руб. Отсюда определяем % недостатка средств:

(10)

Подставив полученные значения в формулы (7)-(9) находят величину общего риска после внедрения мер.

Аналогично выполняются расчеты для следующих *N*-1 способов распределения выделенных средств, после чего выбирается минимальный общий риск угроз.

*1-й способ распределения:*

На файерволл – 8000 руб., система назначения паролей – 0 руб.

*2-й способ распределения*

На файерволл – 6000 руб., система назначения паролей – 2000 руб.

***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.

;

.

***Задание 2.6.*** Найти критичность реализации угрозы 1 через уязвимость 1 (*ER1/1*), т.е. степень влияния однократной реализации угрозы 1 на среднюю работоспособность всех пяти информационных активов системы. Определить для выявленных угроз и уязвимостей:

* уровень угрозы 1 по уязвимости 1(*Th1/1*);
* уровень угрозы 1 по уязвимости 2(*Th1/2*);
* уровень угрозы 2 по уязвимости 1(*Th2/1*);
* уровень угрозы 2 по уязвимости 2(*Th2/2*);
* уровень угрозы 1 по всем (двум) уязвимостям (*CTh1*); – уровень угрозы 2 по всем (двум) уязвимостям (*CTh2*).

Критичность реализации угрозы 1 через уязвимость 2 составляет 20 %; угрозы 2 через уязвимость 1 – 30 %; угрозы 2 через уязвимость 2 – 40 %. Вероятности реализации

угроз через каждую из уязвимостей (*P(V)*) считать равновероятными, т.е. 50%.

***Задание 2.7.*** На основании полученных результатов сделать вывод о целесообразности проведения мер противодействия выявленным угрозам, и указать категории контрмер (см. страница 3), к которым можно отнести предлагаемые методы парирования из пятого этапа.