БГУИР

Кафедра ЗИ

Отчёт

По практическому занятию №3

По теме:

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнили: Проверил:

Студенты гр. 153502 Столер Д.В.

Савончик Е.В.

Логвинов А.С.

Глытов П.С.

Андреевский И.Э.

Минск 2022

**Цель работы:** 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, 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.

**Уязвимость 1:** Отсутствие антивирусного ПО.

**Уязвимость 2:** Скачивание одним из работников зараженного файла из ненадежного источника.

**Угроза 2**:

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

**Уязвимость 1:** Информация хранится в незащищенном формате.

**Уязвимость 2:** Прослушивание и перехватывание разными способами каналов связи.

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

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

***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 (минимума риска)?» требуется оптимально распределить средства годового бюджета (8000 руб.) на парирование угрозы 1 и парирование угрозы 2

1. Фаервол – 8000 руб, система назначения паролей – 0 руб.
2. Фаервол – 7000 руб, система назначения паролей – 1000 руб.
3. Фаервол – 6000 руб, система назначения паролей – 2000 руб.

Третий вариант распределения является наиболее оптимальным

***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:

**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 фаервол. Используемые контрмеры относятся к категориям обеспечения безопасности на сетевом уровне и на уровне системного администратора.