БГУИР

Кафедра ЗИ

Отчёт

по практическому занятию №2

по теме: «Анализ рисков информационной безопасности»

Выполнили Проверил:

студенты группы 950501: Столер Д.В

Деркач А.В.

Романчук А.В.

Минск 2021

1. **Исходные данные для выполнения**

*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 информацию.

1. **Выполнение практического задания**

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



Данные для расчета были взяты из этапа 2 и 4.

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



Данные для расчета были взяты из этапа 2 и 4.

***Задание 2.3.*** Найти РИСКобщий.



где  — ЦЕНАущерба по i-й угрозе;

 — ВЕРОЯТНОСТЬущерба (весовой коэффициент) i-й угрозы, выбираемый экспертами из условия:



***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.

Рассчитаем РИСК по 1-й угрозе:



Рассчитаем РИСК по 2-й угрозе:



Далее мы рассмотрим 3 способа распределения средств бюджета (8000 руб.). Для этого мы будем пользоваться следующими формулами:

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



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:



где R2 – РИСК по 2-й угрозе, руб.;

Общий риск угроз после внедрения мер должен быть минимально возможным:



Рассмотрим 1-й способ (8000 руб. на фаерволл, тогда на систему назначения паролей остается – 0 руб.):



Рассмотрим 2-й способ (7000 руб. на фаерволл, тогда на систему назначения паролей остается – 1000 руб.):



Рассмотрим 3-й способ (6000 руб. на фаерволл, тогда на систему назначения паролей остается – 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.



Наиболее эффективным является = 82,2%

***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).

Для расчета будем использовать следующие формулы:

Уровень угрозы по уязвимости (Th):



где ER (критичность реализации угрозы) — степень влияния реализации угрозы на ресурс, т.е. как сильно повлияет угроза на работу ресурса;

P(V) (вероятность реализации угрозы через данную уязвимость) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях.

На основании значений уровней угроз по уязвимости осуществляется расчет по всем уязвимостям, по которым реализуется данная угроза (CTh):



Найдем критичность реализации угрозы 1 через уязвимость 1 (ER1/1):



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 %. Произведем расчеты:

Уровень угрозы 1 по уязвимости 1 ():



Уровень угрозы 1 по уязвимости 2 ():



Уровень угрозы 2 по уязвимости 1 ():



Уровень угрозы 2 по уязвимости 2 ():



Уровень угрозы 1 по двум уязвимостям ():



Уровень угрозы 2 по двум уязвимостям ():



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

Исходя из полученных расчетов, проведение мер противодействия выявленным угрозам целесообразно т.к. эффективность принятых мер безопасности 82%, что является довольно высоким показателем.

Категории контрмер, к которым можно отнести предлагаемые методы парирования, следующие:

- обеспечение безопасности на сетевом уровне;

- обеспечение безопасности поддерживающей инфраструктуры.