БГУИР

Кафедра ЗИ

Отчёт

по практическому занятию № 2

по теме: «Анализ рисков информационной безопасности»

Выполнили Проверил

студенты группы № 950503 Столер, Д.В.

Гуринович, А.В

Сякачёв, П.В.

Минск 2021

**Вариант № 7**

**Задание № 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.

**Задание № 2. Стоимость информационных активов.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Актив | 1 | 2 | 3 | 4 | 5 |
| Стоимость, руб. | 700 | 500 | 3200 | 9000 | 500000 |

**Задание № 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 № 4. Количественные оценки рисков.**

1. Цена ущерба по угрозе 1 составила:

рублей в год.

1. Цена ущерба по угрозе 2 составила:

50600 рублей в год.

1. Общий риск от обеих угроз:

,

где – вероятность ущерба для угрозы 1 (, – вероятность ущерба для угрозы 2 (;

= 43820 рублей за год

**Задание № 5. Выбор методов парирования угроз.**

* 1. Распределение средств годового бюджета.

**Случай 1.** 8000 рублей на firewall, 0 рублей на систему назначения паролей.

Rост.1 = R1 \* x/100 = p1 \* U1 \* x/100 = 0.60 \* 39300 \* 11 / 100 = 2593.8 (руб)

Rост.2 = R2 \* y/100 = p2 \* U2\* x/100 = 0.40 \* 50600 \* 100 / 100 = 20240 (руб)

Rпосле внед.мер = ( Rост.1 + Rост.2) = 22833.8 (руб)

**Случай 2.** 7000 рублей на firewall, 1000 рублей на систему назначения паролей.

Rост.1 = R1 \* x/100 = p1 \* U1 \* x/100 = 0.60 \* 39300 \* 22 / 100 = 5187.6 (руб)

Rост.2 = R2 \* У/100 = p2 \* U2\* x/100 = 0.40 \* 50600 \* 50 / 100 = 10120 (руб)

Rпосле внед.мер = ( Rост.1 + Rост.2) = 15307.6 (руб)

**Случай 3.** 6000 рублей на firewall, 2000 рублей на систему назначения паролей.

Rост.1 = R1 \* x/100 = p1 \* U1 \* x/100 = 0.60 \* 39300 \* 33 / 100 = 7781.4 (руб)

Rост.2 = R2 \* У/100 = p2 \* U2\* x/100 = 0.40 \* 50600 \* 0 / 100 = 0 (руб)

Rпосле внед.мер = ( Rост.1 + Rост.2) = 7781.4 (руб)

Общий риск угроз после внедрения мер минимален в третьем случае.

**Общий риск** – = 43820 руб.

**Минимально возможный риск -** Rпосле внед.мер = 7781.4 руб.

* 1. Оценка эффективности принятых мер (EF).

Эффективность принятый мер безопасности:

Таким образом, после внедрения мер безопасности риск уменьшился на 82.2 %. В денежном эквиваленте риск составит:

рублей

Критичность реализации угрозы 1 через уязвимость 1:

**Задание № 6.**

Найдем 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.

Определим для выявления угроз и уязвимостей (вероятность реализации угроз – 50%).

–  уровень угрозы 1 по уязвимости 1

* уровень угрозы 1 по уязвимости 2, где критичность реализации

20%.

– уровень угрозы 2 по уязвимости 1, где критичность реализации 30%

– уровень угрозы 2 по уязвимости 2, где критичность реализации 40%

– уровень угрозы 1 по всем (двум) уязвимостям

– уровень угрозы 2 по всем (двум) уязвимостям

**Задание № 7. Вывод.**

В результате работы можно сделать вывод, что наиболее эффективным вариантом распределения средств на меры безопасности для парирования обеих угроз является случай № 3, так как при одинаковых для всех трёх случаев затратах в 8000 рублей, общий риск угроз для этого случая снижается на 82,2 процента, в сравнении с двумя другими случаями, это наиболее эффективно и является целесообразной тратой.

Данные меры безопасности относятся к следующим категориям:

* Обеспечение безопасности на сетевом уровне.
* Обеспечение безопасности на уровне системного администратора.