­­Министерство образования Республики Беларусь

Учреждение образования

БелорусскиЙ государственный университет

информатики и радиоэлектроники

Факультет Компьютерных Систем и Сетей

Кафедра Программного обеспечения информационных технологий

|  |
| --- |
|  |
|  |

Практическая работа №3

по дисциплине «Основы защиты информации»

на тему:

Анализ рисков информационной безопасности.

Колличественная оценка информационных рисков

|  |  |  |
| --- | --- | --- |
| Выполнил  Студент гр. 751003 |  | Стубеда В.Д. |
| Проверила: |  | Саванович С.Э. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Минск, 2019

*Этап 1.* Информационные активы системы:

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 системы.

Актив 5. Данные в СУБД.

*Этап 2.* Стоимость ресурсов

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

*Этап 3.* Основные угрозы с наиболее высокими приоритетами:

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.

*Этап 4.* В результате реализации угрозы 1 с вероятностью ущерба 0,6 наступило первое последствие «Финансовые потери, связанные с восстановлением ресурсов», причём вредоносное ПО проникало в сеть организации 6 раз в год и каждый раз повреждало на 100 % активы 1–3 и на 20 % актив 4. Актив 5 был защищён резервным копированием и повреждением его можно пренебречь.

Кроме того, в результате реализации этой угрозы с вероятностью ущерба 0,6 наступило второе последствие «Дезорганизация деятельности компании». За 6-кратное в течение года проникновение вредоносного ПО цена ущерба по этому последствию составила 2100 руб.

В результате реализации угрозы 2 с вероятностью ущерба 0,4 наступило первое последствие «Финансовые потери от разглашения и передачи информации конкурентам». Цена ущерба по этому последствию за год составила 17600 руб.

Кроме того, в результате реализации этой угрозы с вероятностью ущерба 0,4 наступило второе последствие «Ущерб репутации организации». Цена ущерба по этому последствию за счёт уменьшения потока заказов и неприятностей со стороны государственных органов составила 33000 руб. за год.

*Этап 5.* Методом парирования угрозы 1 является закупка определённого набора программных средств (фаерволла, межсетевого экрана), а методом парирования угрозы 2 – разработка и внедрение системы назначения паролей для доступа к информационным активам. Стоимость наилучшего фаерволла – 9000 руб. Стоимость разработки и внедрения наилучшей системы назначения паролей – 2000 руб. Утверждённый годовой бюджет на информационную безопасность составляет 8000 руб.

***Задание 1.*** Финансовые потери, связанные с восстановлением ресурсов:

Актив 1: РИСК = 0,6 \* 1 \* 700 = 420;

Актив 2: РИСК = 0,6 \* 1 \* 500 = 300;

Актив 3: РИСК = 0,6 \* 1 \* 3200 = 1920;

Актив 4: РИСК = 0,6 \* 0,2 \* 9000 = 1080;

Актив 5: РИСК = 0,6 \* 0 \* 500000 = 0;

Дезорганизация деятельности компании:

РИСК = 0,6 \* 2100 = 1260.

R1 = 420 + 300 + 1920 + 1080 + 0 + 1260 = 4980;

***Задание 2.*** Финансовые потери от разглашения и передачи информации конкурентам:

РИСК = 0,4 \* 17600 = 7040;

Ущерб репутации организации:

РИСК = 0,4 \* 33000 = 13200.

R2 = 7040 + 13200 = 20240;

***Задание 3.***

РИСК общий = 420 + 300 + 1920 + 1080 + 0 + 1260 + 7040 + 13200 = 25220.

***Задание 4.***

; =100% ;

;

;

R после внед. мер = (Rост.1 + Rост.2) = 20788.

; =0%;

;

;

R после внед. мер = (Rост.1 + Rост.2) = 1643.

R мин. общий = 1643.

***Задание 5.*** Эффективность принятых мер (в процентах):

E = =93.48%.

***Задание 6.*** Эффективность принятых мер (в процентах):

 

*Th1/1* = 0,32;

*Th1/2* = 0,1;

*Th2/1* = 0,15;

*Th2/2* = 0,2;

*CTh1* = 0,388;

*CTh2* = 0,32.