Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра защиты информации

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Методология информационной безопасности»

для студентов специальности
1-98 01 02 «Защита информации в телекоммуникациях»

Минск 2021

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8
«ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Цель занятия: изучить методику оценки рисков информационной безопасности и получить практические навыки по ее применению.

1 Краткие теоретические сведения

Необходимость обеспечения безопасности информации определяется тем ущербом, который может быть нанесен вследствие ее утечки. В случае если ущерб не является приемлемым, то необходимо его минимизировать за счет использования методов и реализующих их средств защиты информации. Их применение, особенно в информационных системах, требует определения некоторого показателя, который бы позволил оценить эффективность их использования. Данный критерий носит наименование риска информационной безопасности.

Сущность минимизации риска информационной безопасности сводится к получению такого значения остаточного риска, которое является приемлемым для организации. Для того чтобы обеспечить этот процесс необходимо управлять рисками информационной безопасности, что реализуется в соответствии с моделью, изображенной на рисунке 1.

Владелец информационного ресурса (в соответствии с законодательством Республики Беларусь – руководитель организации) стремится его сохранить от несанкционированного доступа (утечка информации в информационных системах). Для этого он использует определенные контрмеры (средства защиты информации), которые позволяют обеспечить снижение риска потери информационного ресурса. Такое стечение обстоятельств усложняют задачу несанкционированного доступа нарушителя к информации и соответственно минимизируют риск потери информационного ресурса его владельцем.

Для того чтобы нарушителю получить несанкционированный доступ в таких условиях ему необходимо найти уязвимость в системе защиты, которая позволит ему достичь цели.

Уязвимость - возможность возникновения на каком–либо этапе жизненного цикла информационной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Таким образом, минимизация риска обусловлена рядом факторов: устранением уязвимостей в информационных системах и использованием средств защиты информации.

Рисунок 1. – Модель управления рисками информационной безопасности

Оценка рисков информационной безопасности выполняется исходя из ниже приведенной методики.

Этап 1. Определяется состав информационных активов информационной системы и ее границы (оборудование, входящее в нее).

Информационный актив – информация вне зависимости от формы ее представления, использование которой в процессе производственной деятельности позволяет организации получать прибыль.

Этап 2. Определяется стоимость информационных активов. Это позволяет оценить их значимость для организации и стоимость их утраты, а также определить необходимость и достаточность предлагаемых средств их защиты.

Этап 3. Оцениваются угрозы безопасности информации и уязвимости информационной системы, посредством которых они могут быть реализованы.

Это приводит к следующим возможным последствиям:

Последствие 1. Ущерб репутации организации.

Последствие 2. Финансовые потери, связанные с восстановлением информационных активов.

Последствие 3. Невозможность деятельности компании вследствие нарушения функционирования ее информационной системы.

Последствие 4. Финансовые потери от разглашения и передачи информации третьим лицам.

Этап 4. Выполняется анализ рисков информационной безопасности, что позволяет оценить потери организации вследствие реализации угроз безопасности информации. Оценка риска информационной безопасности по двум факторам (вероятность возникновения угрозы безопасности информации и цена ущерба) выполняется с использованием следующего выражения:

$$\text{РИСК}=\text{ВЕРОЯТНОСТЬ}_{\text{УГРОЗЫ}}\cdot\text{ЦЕНА}_{\text{УЩЕРБА}} \quad (1)$$

Оценка риска информационной безопасности по трем факторам (вероятность возникновения угрозы безопасности информации, вероятность использования нарушителем некоторой уязвимости, что приводит к реализации некоторой угрозы и цена ущерба) выполняется с использованием следующего выражения:

$$\text{РИСК}=\text{ВЕРОЯТНОСТЬ}_{\text{УГРОЗЫ}}\cdot\text{ВЕРОЯТНОСТЬ}_{\text{УЯЗВИМОСТИ}}\cdot\text{ЦЕНА}_{\text{УЩЕРБА}} \quad (2)$$

Если информационный актив подвержен нескольким (N) угрозам безопасности информации, то общий риск ($\text{РИСК}_{\text{общий}}$) нанесения нарушителем ущерба может быть определен как:

$$\text{РИСК}_{\text{общий}} = \sum_{i=1}^{N} p_i \times U_i , \quad (3)$$

где U_i – $\text{ЦЕНА}_{\text{ущерба}}$ по i-й угрозе; p_i – $\text{ВЕРОЯТНОСТЬ}_{\text{ущерба}}$ (весовой коэффициент) i-й угрозы, выбираемый экспертами из условия:

$$\sum_{i=1}^{N} p_i = 1 \quad (4)$$

Этап 5. Реализуется управление рисками. На этом этапе выбираются средства защиты информации, которые позволят снизить риск.

При анализе риска информационной безопасности используют следующие термины:

Критичность реализации угрозы (ER) – степень влияния угрозы безопасности информации на информационный актив (конфиденциальность, целостность, доступность, сохранность, подлинность).

Вероятность реализации угрозы безопасности информации через определенную уязвимость (P(V)) – определяет вероятность реализации угрозы безопасности информации через определенную уязвимость информационной системы.

Учитывая эти термины, определяется уровень угрозы по уязвимости (*Th*):

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}. \quad (5)$$

На основании значений уровня угрозы по уязвимости осуществляется расчет по всем уязвимостям, по которым реализуется данная угроза (*CTh*):

$$Cth = 1 - \prod_{i=1}^{n} (1 - Th_n). \quad (6)$$

Рассмотрим пример. Пусть проводится оценка рисков информационной безопасности следующей информационной системы (рисунок 2).

Архитектура информационной системы следующая:

– рабочие места (РМ) ввода информации – персональные компьютеры, на которых пользователи обрабатывают информацию;

– почтовый сервер, на который информация поступает с удаленных узлов сети через сеть Интернет и по ведомственным каналам связи (ВКС);

– сервер обработки информации и СУБД – используется для хранения информации в базе данных, взаимодействия пользователей с которой осуществляется через систему управления базами данных (СУБД);

– сервер резервного копирования – предназначенный для хранения резервных копий базы данных и ее восстановления в случае сбоя сервера обработки и СУБД;

– рабочие места группы оперативного резерва – персональные компьютеры, на которых пользователи обрабатывают информацию в случае выхода из строя рабочих мест ввода информации;

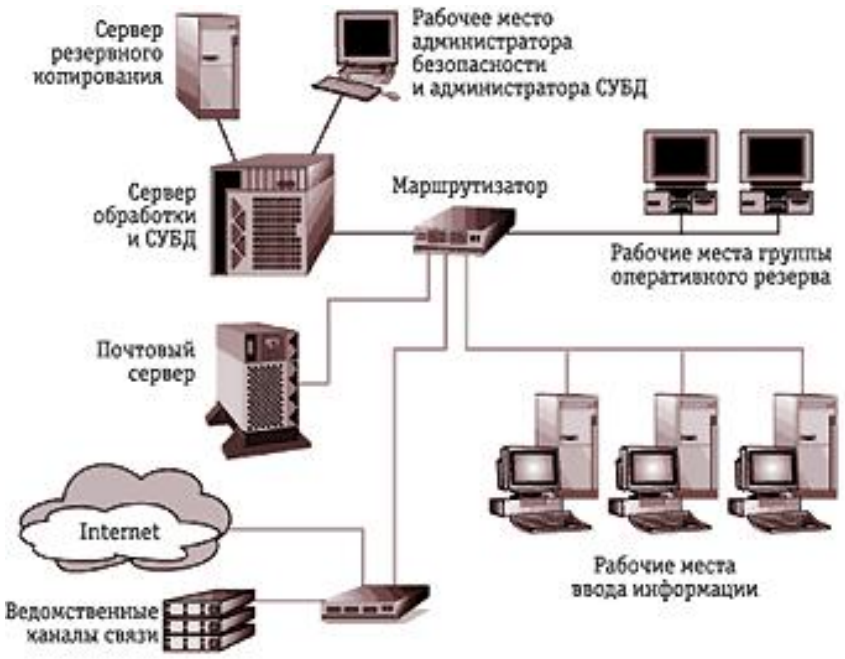

Рисунок 2. – Архитектура информационной системы

– рабочее место администратора безопасности и администратора СУБД - персональный компьютер, предназначенный для настройки и технической эксплуатации информационной системы.

Функционирование информационной системы осуществляется следующим образом. Данные, введенные с РМ пользователей, поступившие на почтовый сервер из сети Интернет и из ВКС направляются на сервер обработки данных и СУБД.

2 Практическое задание

Проанализируем риски информационной безопасности информационных активов информационной системы (рисунок 2) с помощью вышеизложенной методики.

Этап 1. Определение границ информационной системы. Для этого определим состав информационных активов. Допустим, что информационными активами являются следующие:

Актив 1. Данные, поступившие на сервер обработки и СУБД из сети Интернет.

Актив 2. Данные, поступившие на сервер обработки и СУБД из ВКС.

Актив 3. Данные, поступившие на сервер обработки и СУБД с РМ пользователей.

Актив 4. Системное и прикладное программное обеспечение.

Актив 5. Данные, хранимые в базе данных.

Этап 2. Стоимость информационных активов

Наименование актива	Актив 1	Актив 2	Актив 3	Актив 4	Актив 5
Стоимость актива, тыс. руб.	7	5	32	1000	50000

Этап 3. На основании анализа особенностей обработки информации в информационной системе определены следующие угрозы безопасности информации:

Угроза 1. Загрузка из сети Интернет в информационную систему вредоносной программы обусловленная непреднамеренными действиями сотрудника организации.

Угроза 2. Передача информации сотрудником организации третьим лицам, который имеет к ней легальный доступ.

Этап 4. Пусть в результате реализации *угрозы 1* с вероятностью 0,6 наступило последствие «Финансовые потери, связанные с восстановлением информационных активов». Вредоносная программа загружалась в информационную систему 6 раз за год и каждый раз повреждала на 100 % активы 1–3 и на 30 % актив 4, что обуславливает критичность реализации *угрозы 1* через *уязвимость 1* этой информационной системы. Актив 5 был защищён резервным копированием и его повреждением можно пренебречь.

Кроме того, в результате реализации этой угрозы наступило последствие «Невозможность деятельности компании вследствие нарушения функционирования ее информационной системы». Пусть за 6-кратную в течение года загрузку вредоносной программы цена ущерба по этому последствию составила 21 тыс. руб.

В результате реализации *угрозы 2* с вероятностью 0,4 наступило последствие «Финансовые потери от разглашения и передачи информации третьим лицам». Пусть цена ущерба составила 56 тыс. руб.

Кроме того, в результате реализации этой угрозы наступило последствие «Ущерб репутации организации». Пусть цена ущерба за счёт уменьшения потока заказов составила 88 тыс. руб.

Этап 5. Выбор методов и средств минимизации угроз. Для противодействия *угрозе 1* необходимо использовать средство защиты информации - антивирус, а для противодействия *угрозе 2* – разработать и внедрить систему парольной защиты для доступа к информационным активам организации. Стоимость наилучшего по техническим параметрам антивируса – 90 тыс. руб. Стоимость разработки и внедрения наилучшей системы парольной защиты – 20 тыс. руб. Утверждённый годовой бюджет на информационную безопасность в организации составляет 80 тыс. руб. Для принятия решения о рациональном распределении финансовых средств необходимо выполнить оценку рисков.

Задание 1. Найти цену ущерба при реализации *угрозы 1*.

Задание 2. Найти цену ущерба при реализации *угрозы 2.*

Задание 3. Найти общий риск при реализации *угрозы 1* и *угрозы 2*.

Задание 4. Исходя из размера выделенного годового бюджета на информационную безопасность в организации, необходимо минимизировать остаточный риск информационной безопасности за счет оптимального распределения средств (80 тыс. руб.) на противодействие *угрозе 1* и противодействие *угрозе 2*, считая, что для рассматриваемой информационной системы экспертным путём установлено, что:

– недостаток каждых x % средств от стоимости наилучшего антивируса позволяет приобрести менее дорогой антивирус, обуславливающий, однако, риск реализации угрозы безопасности информации исчисляемый в денежном эквиваленте в размере:

$$584,4 \times \frac{x}{100} \text{ [тыс. руб.]} \qquad (7)$$

– недостаток каждых y % средств от стоимости наилучшей системы парольной защиты позволяет приобрести менее дорогую систему, обуславливающую, однако, риск реализации угрозы безопасности информации исчисляемый в денежном эквиваленте в размере:

$$141,6 \times \frac{y}{100} \text{ [тыс. руб.]} \qquad (8)$$

Задание 5. Оценить эффективность принятых мер для противодействия угрозам безопасности информации по формуле:

$$E = \frac{РИСК_{общий} - РИСК_{остаточный}}{РИСК_{общий}} \times 100\% \quad (9)$$

Задание 6. Найти критичность реализации *угрозы 1* через *уязвимость 1*. Определить для всех отмеченных выше угроз и уязвимостей *Th* и *CTh*, если критичность реализации *угрозы 1* через *уязвимость 2* составляет 20 %; *угрозы 2* через *уязвимость* 1 – 40 %; *угрозы 2* через *уязвимость 2* – 30 %. Реализацию угроз безопасности информации через каждую из уязвимостей считать равновероятными.

3 Контрольные вопросы

1. В чем заключается сущность минимизации риска информационной безопасности?
2. За счет чего можно минимизировать риск информационной безопасности?
3. Что такое информационный актив?
4. Каким образом оценивается риск?
5. Что является критерием эффективности принятых мер для противодействия угрозам безопасности информации?