МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет информационных технологий и робототехники (ФИТР)

Кафедра программного обеспечения вычислительной техники

и автоматизированных систем

**О Т Ч Е Т**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

# «ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ»

|  |  |
| --- | --- |
| Выполнил: | Ст. гр. 10701322 Свиржевская В. В.  Махонина Ю. В. |
| Проверил: | Давыденко Н. В. |

Минск 2024

**Цель работы:** познакомиться с моделями безопасности и существующими методиками оценки рисков.

**Условие**

**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 пользователей.

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 | 100000 | 5000000 |

**Этап 3.** Определение угроз.

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.

Существующие уязвимости:

Уязвимость 1. Отсутствие антивирусного ПО и брандмауэра.

Уязвимость 2. Слабый контроль за назначением паролей пользователей.

Пусть в результате реализации угрозы 1 с вероятностью 0,6 наступило 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 30% актив 4. Актив 5 был защищён резервным копированием и повреждением его можно пренебречь.

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

Пусть в результате реализации угрозы 2 с вероятностью 0,4 наступило последствие «Финансовые потери от разглашения и передачи информации конкурентам». Цена ущерба по этому последствию составила 5600 руб.

Кроме того, в результате реализации этой угрозы наступило последствие «Ущерб репутации организации». Цена ущерба по этому последствию за счёт уменьшения потока заказов и неприятностей со стороны государственных органов составила 8800 руб.

**Этап 5.** Выбор методов парирования угроз. Пусть методом парирования угрозы 1 является закупка определённого набора программных средств фаерволла (брандмауэра), а методом парирования угрозы 2 – разработка и внедрение системы назначения паролей для доступа к информационным активам.

Стоимость наилучшего брандмауэра – 9000 руб.

Стоимость разработки и внедрения наилучшей системы назначения паролей – 2000 руб.

Утверждённый годовой бюджет на информационную безопасность составляет 8000 руб.

**Задание 1**

Найти цену ущерба по угрозе 1.

**Получившийся результат**

ЦЕНАущерба = 6\*(700+500+3200+100000\*0,3)+2100 = 208500 руб.

**Задания 2**

Найти цену ущерба по угрозе 2.

**Получившийся результат**

ЦЕНАущерба = 5600+8800 = 14400 руб.

**Задание 3**

Найти суммарный риск для информационной системы - РИСКобщий.

**Получившийся результат**

РИСКобщий = 0,6\*(208500-2100)+0,4\*14400+0,6^6\*2100 = 129697,98 руб.

**Задание 4**

Исходя из критерия «Как, оставаясь в рамках утвержденного годового бюджета на информационную безопасность достигнуть максимального уровня защищенности информационных активов компании (минимума риска)?» оптимально распределить выделенные средства на парирование угроз, считая, что для рассматриваемой корпоративной информационной системы экспертным путём установлено, что:

– недостаток каждых *х*% средств от стоимости наилучшего брандмауэра позволяет приобрести более дешёвый брандмауэр, оставляющий, однако, риск угрозы в размере:

|  |  |
| --- | --- |
| [руб.] | (2.7) |

– недостаток каждых *у*% средств от стоимости наилучшей системы назначения паролей позволяет приобрести более дешёвую систему, оставляющую, однако, риск угрозы в размере:

|  |  |
| --- | --- |
| [руб.] | (2.8) |

Определить значение оставшегося суммарного риска для информационной системы после парирования угроз (РИСКобщий ост).

**Получившийся результат**

Требуется купить более дешевый брандмауэр ценой в 6000 руб. и наилучшую систему назначения паролей за 2000 руб.

РИСКобщий ост = 58440\*((9000-6000)/9000)+14160\*((2000-2000)/2000) = 19480 руб.

**Задание 5**

Оценить (в процентах) эффективность принятых мер для парирования угроз, т.е. найти отношение (РИСКобщий - РИСКобщий ост)/ РИСКобщий\*100%.

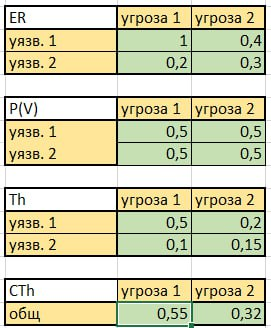
**Получившийся результат**

(РИСКобщий - РИСКобщий ост)/ РИСКобщий\*100% = (129697,98 – 19480) / 129697,98 \* 100% = 84,98%

**Задание 6**

Для всех выявленных угроз и уязвимостей определить уровень угрозы по уязвимости **(***Th*) и уровень угрозы по всем уязвимостям (*CTh*), если критичность реализации угрозы 1 через уязвимость 1 (*ER*) составляет 100%, критичность реализации угрозы 1 через уязвимость 2 составляет 20%; угрозы 2 через уязвимость 1 – 40%; угрозы 2 через уязвимость 2 – 30%. Реализации угроз через каждую из уязвимостей считать равновероятными.

**Получившийся результат**



**Контрольные вопросы:**

1. Что такое информационная безопасность, защита информации?

**Информационная безопасность** – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений (владельцам и пользователям информации и поддерживающей инфраструктуры).

**Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

1. Какие модели безопасности вы знаете? Опишите их.

Понятие информационной безопасности может быть пояснено с помощью **моделей безопасности.**

Система считается безопасной, если она может противостоять нарушениям. Но нарушений безопасности может быть очень много. Суть моделей безопасности в том, что множество всех видов нарушений безопасности делится на несколько базовых групп. Затем любое из нарушений относится к одной из групп. Если система может противостоять любой из групп нарушений, то она считается безопасной.

Одной из первых и наиболее популярных моделей безопасности является **модель «Триада КЦД»** (Конфиденциальность, Целостность, Доступность) или в англоязычной форме – **CIA** (Confidentiality, Integrity, Availability).

Популярными моделями безопасности являются **«Гексада Паркера» и модель STRIDE,** используемая компанией Microsoft для разработки безопасного ПО.

1. Что понимается под конфиденциальностью, доступностью, целостностью?

Под конфиденциальностью, доступностью, целостностью понимаются базовые группы нарушений, которые помогают определить безопасность системы. Если система может противостоять любой из групп нарушений, то она считается безопасной.

1. Дайте определения терминам: уязвимость, угроза, атака, риск.

**Уязвимость** – это слабое звено информационной системы.

Например:

- сбои и отказы оборудования ИС;

- последствия ошибок проектирования и разработки компонентов ИС: аппаратных средств, технологий обработки информации, алгоритмов, программ, структур данных и т.п. (ошибка в программе, использование слабого алгоритма шифрования)

- ошибки настройки и эксплуатации (примитивный пароль, неправильное назначение прав доступа к файлу с важными данными)

**Угроза** – потенциальная возможность нарушить информационную безопасность (конфиденциальность, целостность, доступность информации).

**Атака** – реализованная угроза.

Атака может произойти только тогда, когда одновременно существуют уязвимость и направленная на использование этой уязвимости угроза.

**Риск** – вероятностная оценка величины возможного ущерба, который может понести предприятие в результате успешно проведенной атаки.

1. Как и по каким критериям можно классифицировать угрозы?

Критерий 1. Ущерб репутации организации.

Критерий 2. Финансовые потери, связанные с восстановлением ресурсов.

Критерий 3. Дезорганизация деятельности компании.

Критерий 4. Финансовые потери от разглашения и передачи информации конкурентам, а также другие критерии.

1. Приведите известные вам примеры атак.

DDoS – атака.

1. Что такое управление рисками? Какие этапы включает управление рисками?

**Управление рисками** – это системный анализ угроз, прогнозирование и оценка их последствий для предприятия и выбор контрмер, направленных на уменьшение возможного негативного воздействия нарушений на деятельность предприятия.

Управление рисками включает 3 этапа:

1. Анализ уязвимостей;
2. Оценка рисков;
3. Риск-менеджмент.

**Анализ уязвимостей** – объективное исследование реально существующих активов предприятия, являющихся объектом защиты: оборудования, сети, ПО, документации, баз данных. Выявление уязвимостей и возможных угроз.

**Оценка рисков** – ранжирование возможных угроз по степени опасности. Вычисление рисков (чем выше ущерб и вероятность, тем больше риск).

**Риск-менеджмент** – принятие конкретных мер (разработка и внедрение политики безопасности предприятия).

По каждому риску предпринимаются меры из списка:

- Принятие риска. Касается неизбежных атак, наносящих приемлемый ущерб.

- Устранение риска. Существующий риск сводится на нет либо устранением уязвимости (исправить ошибку), либо угрозы (установить антивирус).

- Снижение риска. Если риск невозможно ни принять, ни устранить, то предпринимаются действия по его снижению (более строгие требования к паролям).

- Перенаправление риска. Если невозможно вышеизложенное, то риск может быть перенаправлен страховой компании.

1. Какие существуют методики оценки рисков и управления ими? Опишите этапы методики оценки рисков CRAMM.

Методики управления рисками делятся на количественные и качественные.

**Качественные методики управления рисками** приняты на вооружение в технологически развитых странах многочисленной армией внутренних и внешних IT-аудиторов. Эти методики достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 17799–2002.

К качественным методикам управления рисками относятся методики *COBRA* и *RA Software Tool*.

**Количественные методики управления рисками** по сути сводятся к поиску единственного оптимального решения из множества существующих. Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного *WWW* сайта или корпоративной *e-mail*) выбрать с учетом известных ограничений бизнес-ресурсов компании?»

К количественным методикам управления рисками относятся методики *CRAMM*, *DREAD*, *RiskWatch, MethodWare* и др.

**Методика *CRAMM****.*

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа.

Управление рисками осуществляется в несколько этапов.

Первый этап **-** инициализации – «*Initialization*» – определяются границы исследуемой информационной системы компании, состав и структура ее основных физических и информационных активов и транзакций. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

На этапе 2 идентификации и оценки ресурсов – «*Identification and Valuation of Assets*» – четко идентифицируются активы и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На этапе 3 оценивания угроз и уязвимостей – «*Threat and Vulnerability Assessment*» – идентифицируются и оцениваются угрозы и уязвимости информационных активов компании. Для такой оценки и идентификации в коммерческом варианте метода *СRAMM* (профиль *Standard*, в других вариантах совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения) используется следующая совокупность критериев (последствий реализации угроз информационной безопасности).

Критерий 1. Ущерб репутации организации.

Критерий 2. Финансовые потери, связанные с восстановлением ресурсов.

Критерий 3. Дезорганизация деятельности компании.

Критерий 4. Финансовые потери от разглашения и передачи информации конкурентам, а также другие критерии.

Этап 4 анализа рисков – «*Risk Analysis*» – позволяет получить количественные оценки рисков. Эти оценки могут быть рассчитаны по формулам (2.1) – (2.4)

На этапе 5 управления рисками – «*Risk management*» – предлагаются меры и средства уменьшения или уклонения от риска. Возможно проведение коррекции результатов или использование других методов оценки. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

На заключительной стадии *CRAMM* генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

– обеспечение безопасности на сетевом уровне;

– обеспечение физической безопасности;

– обеспечение безопасности поддерживающей инфраструктуры;

– меры безопасности на уровне системного администратора.

1. Как вычислить значение риска по определенной угрозе? Как вычислить совокупный риск нанесения злоумышленниками ущерба информационной системе?

Согласно ГОСТ Р 51897-2002 риск – это сочетание вероятности события и его последствий, а его величина РИСК может быть вычислена по формулам:

|  |  |
| --- | --- |
| РИСК=ВЕРОЯТНОСТЬущерба·ЦЕНАущерба |  |

|  |  |
| --- | --- |
| РИСК=ВЕРОЯТНОСТЬугрозы·ВЕРОЯТНОСТЬуязвимости·ЦЕНАущерба |  |

Если информационный объект (ИО) подвержен нескольким (*N*) угрозам (критериям оценки возможного ущерба) то совокупный РИСКобщий нанесения злоумышленниками ущерба ИО может быть представлен как

|  |  |
| --- | --- |
| , |  |

где *Ui* – ЦЕНАущерба по *i*-й угрозе;

*рi* – ВЕРОЯТНОСТЬущерба (весовой коэффициент) *i*-й угрозы, выбираемый экспертами из условия:

|  |  |
| --- | --- |
|  |  |

Методики управления рисками делятся на количественные и качественные.

1. Что такое критичность реализации угрозы?

**Критичность реализации угрозы (*ER*)** – степень влияния реализации угрозы на ресурс, т.е. как сильно повлияет угроза на работу ресурса.

**Выводы:**

Мы на практике ознакомились с тем, как возможно рассчитать риски, оценить эффективности мер, принятых для парирования угроз, оценили уровни угроз по всем уязвимостям и уровни угроз самих уязвимостей; рассмотрели различные методики управления рисками.