Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра защиты информации

Паспорт
расчетно-графического задания (работы)

по дисциплине «Безопасность и защита информации в информационных системах», 3 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны провести анализ предоставленного (выбранного самостоятельно) объекта информатизации, малого предприятия и.т.д., провести оценку рисков и анализ угроз информационной безопасности, обосновать результаты расчетов, предоставить способы устранения выявленных угроз безопасности.

Обязательные структурные части РГЗ.

1) Анализ объекта;
2) Оценка рисков;
3) Анализ угроз;
4) Предложение способов защиты;

Оцениваемые позиции:

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, нет соответствия требованиям к работе, оценка составляет 0 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта проведен куце, недостаточно обоснованы результаты, оценка составляет 15 – 20 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, достаточно обоснованы результаты расчетов, проведен анализ и оценка рисков, не представлены способы устранения недостатков, оценка составляет 20 - 25 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, достаточно обоснованы результаты расчетов, проведен анализ и оценка рисков, представлены способы устранения выявленных недостатков, оценка составляет 25- 30 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

1. Для предприятия малого бизнеса провести:

- Анализ объекта,
- Оценка рисков;
- Анализ угроз;
- Предложение по введению способов и средств защиты;

5. Пример выполнения РГЗ

Оценка рисков и анализ угроз ИБ предприятия:

Специалистами фирмы IBM[2] предложена следующая эмпирическая зависимость ожидаемых потерь от i-ой угрозы информации:

$$Ri=10(Si+Vi-4),$$

где Si – коэффициент, характеризующий возможную частоту возникновения существующей угрозы; Vi – коэффициент, характеризующий значение возможного ущерба при её возникновении. Предложенные специалистами значения коэффициентов следующие:

Таблица 9 - Значения коэффициента Si для расчёта зависимости ожидаемых потерь

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно, 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 10 - Возможные значения коэффициента Vi для расчёта зависимости ожидаемых потерь

Значения возможного ущерба при проявлении угрозы, долл.	Предполагаемое значение Vi
1	0
10	1
100	2
1000	3
10000	4

100000	5
1000000	6
10000000	7

Суммарная стоимость потерь определяется формулой:

$$R = \sum_{\forall i} R_i .$$

На основании предложенной эмпирической формулы рассчитаем число ожидаемых потерь для незащищённой, частично-защищённой и защищённой систем, где незащищённая система – система, не содержащая средств защиты от НСД; частично-защищённая система- имеются средства антивирусной защиты и установлены пароли на вход в систему); защищённая система – система, где установлены средства защиты, перекрывающие возможные каналы утечки информации с некоторым запасом прочности.

Незащищённая система:

1. Потери от компьютерных вирусов

В данной системе средства вычислительной техники заражаются компьютерными вирусами в среднем 1-2 раза в неделю, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(6+3-4) =105=100000$.

2. Потери от взлома пароля (пароль 4 символа, используются 70 знаков).

Взлом происходит в среднем 3 раза в день, ущерб составляет 100$.

Ri=10(7+2-4) =105=100000$.

3. Потери от взлома криптографической защиты.

Взлом происходит в среднем один раз в месяц, ущерб составляет 10000$.

Ri=10(5+4-4) =105=100000$.

4. Потери от DOS-атак (сбой или отказ ИС).

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

5. Потери от троянских программ.

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

6. Потери от логических бомб.

Атаки происходят в среднем 1 раз в месяц, ущерб составляет 10$.

Ri=10(5+1-4)=102=100$.

7. Потери от перехвата информации (подключение к сети).

Несанкционированное подключение происходит 1-2 раза в неделю, ущерб составляет 10$.

Ri=10(6+1-4)=103=1000$.

8. Потери от срыва связи.

Срыв связи в результате действий злоумышленника происходит примерно 1 раз в месяц, ущерб составляет 10$.

Ri=10(5+1-4)=102=100$.

9. Потери от перехвата злоумышленником ПЭМИН.

Примерно 1 раз в 10 лет, ущерб составляет 1000$.

Ri=10(3+3-4)=102=100$.

Суммарная стоимость потерь незащищённой системы будет равна:

$$R = \sum_{\forall i} R_i = 303300\$$$

.

Частично защищённая система (уже существующая):

1. Потери от компьютерных вирусов.

В данной системе при использовании антивирусного средства, средства вычислительной техники заражаются компьютерными вирусами в среднем 1 раз в месяц, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(5+3-4)=104=10000$.

2. Потери от взлома пароля (пароль 7 символов, используется 70 знаков).

При использовании пароля в 7 символов, вероятность подбора пароля составит 1 раз в месяц, ущерб составляет 100$.

Ri=10(5+2-4)=103=1000$.

Остальные элементы, подлежащие защите аналогичны защищённой системе.

Суммарная стоимость потерь частично защищённой системы будет

$$R = \sum_{\forall i} R_i = 12140\$$$

.

Защищённая система:

1. Потери от компьютерных вирусов.

В данной системе при использовании антивирусного средства, средства вычислительной техники заражаются компьютерными вирусами в среднем 1 раз в год, и при этом организации наносится ущерб, равный в среднем 1000$. На основании вышеприведённых таблиц

Ri=10(4+3-4)=103=1000$.

2. Потери от взлома пароля (пароль 8 символов, используются 70 знаков).

При использовании различного рода биометрических датчиков и цифровых ключей, вероятность подбора пароля составит 1 раз в 100 лет, ущерб составляет 100$.

Ri=10(2+3-4) =101=10$.

3. Потери от взлома криптографической защиты.

При использовании средств криптографической защиты, вероятность взлома составит в среднем 1 раз в 10 лет, ущерб составляет 10000$.

Ri=10(3+4-4) =103=1000$.

4. Потери от DOS-атак (сбой или отказ ИС).

При использовании firewalla атаки происходят в среднем 1 раз в 10 лет, ущерб составляет 100$.

Ri=10(3+2-4)=101=10$.

5. Потери от троянских программ.

При использовании средств антивирусной защиты, атаки происходят в среднем 1 раз в год, ущерб составляет 100$.

Ri=10(4+2-4)=102=100$.

6. Потери от логических бомб.

При использовании средств антивирусной защиты, атаки происходят в среднем 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

7. Потери от перехвата информации (подключение к сети).

При использовании VPN, несанкционированное подключение происходит 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

8. Потери от срыва связи.

При использовании firewalla и административных мер, срыв связи в результате действий злоумышленника происходит примерно 1 раз в год, ущерб составляет 10$.

Ri=10(4+1-4)=101=10$.

Суммарная стоимость потерь защищённой системы будет равна:

$$R = \sum_{\forall i} R_i = 2150\$$$.

Эквивалентный выигрыш средств от установки дополнительных СЗИ в незащищенной сети составляет:

$$\Delta = 303300 - 2150 = 301150\$$$.

Эквивалентный выигрыш средств от установки дополнительных СЗИ частично защищенной сети составляет:

$$\Delta = 12140 - 2150 = 9990\$$$.

Анализ риска завершается составлением и принятием ПБ. Она оформляется в виде документа, в общем виде (без излишней детализации) определяющего задачи в области защиты и особенности процесса защиты ресурсов. ПБ определяет стратегию и тактику построения системы безопасности компании. В российской терминологии документ, определяющий стратегию, называют концепцией, а документ, определяющий тактику, - политикой. На Западе принято создавать единый документ, включающий в себя оба аспекта.

ПБ отражает причины, по которым организация использует подключение к открытой, общедоступной сети, и определяет перечень сервисов, предоставляемых всем внутренним и внешним пользователям внутри и вне интранета организации.

На втором этапе с учетом составленной ПБ и согласно полученным решениям составляется план обеспечения ИБ (иногда он называется планом защиты) - официальный документ, описывающий конкретные действия по реализации средств поддержания безопасности системы, который регулярно пересматривается и при необходимости корректируется.

План защиты содержит следующие разделы.

1. Текущее состояние - описание существующей на момент подготовки плана системы защиты.

2. Рекомендации - выбор основных мер, средств и способов защиты, реализующих ПБ для интранета. Будем называть этот комплекс мер системой безопасности. Здесь очень важно установить компромисс между ее ценой и удобством использования. В зависимости от желаемого уровня безопасности и выбранного способа защиты интранета могут потребоваться дополнительные аппаратные средства: маршрутизаторы и выделенные хосты, специальное ПО, а также ставка эксперта по безопасности. Что и составляет

максимальную сумму на установку дополнительных СЗИ.

Для примера рассмотрим, общую стоимость защиты для ОИ, применительно к учебному городку №1 ВАИУ (г. Воронеж).

Для организации защищенного ОИ в качестве системы защиты информации выберем Secret Net v. 4.0 стоимостью 980$. Также необходимо выбрать межсетевой экран Symantec Client Security 3.1 СТОИМОСТЬЮ 57$

Для защиты серверов от вирусных программ применяем программу Dr. Web для Windows - Антивирус +Антиспам стоимостью 166 $.

Для предотвращения от взлома криптографической защиты серверов служб применим средство криптозащиты "УКДС-С" стоимостью 740 $.

Средства VPN для защиты системы от несанкционированного подключения устанавливать не будем в связи с их дороговизной (более 2000$ за 1 комплект) и тем, что межсетевые экраны реализуют большинство способов зашиты, реализуемых в VPN путем специальных настроек.

Суммарная стоимость средств защиты ОИ составляет:

$$\sum = 980 + 57 + 166 + 740 = 1061\$$$

3. Ответственность - список ответственных сотрудников и разграничение сфер их деятельности.

4. Расписание - определение порядка работы механизмов защиты, в том числе и средств контроля.

5. Пересмотр положений плана защиты с указанием периода пересмотра.