УДК 681.3

В.И. Лащевский, Д.А. Зеленков

УЩЕРБНО-ЗАТРАТНАЯ МОДЕЛЬ ЗАЩИТЫ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Рассмотрена ущербно-затратная модель защиты локальной вычислительной сети. Модель позволяет концептуально определить стратегию защиты и оптимальный с экономической точки зрения набор средств защиты. Приведен практический метод определения степени риска безопасной локальной сети.

Известно, что наиболее адекватная оценка эффективности системы защиты информации (СЗИ) может быть получена только тогда, когда в качестве интегрального показателя используют размер ущерба (потерь) вследствие воздействия различных угроз безопасности информации (БИ). В этом случае можно сравнить реальную опасность угроз, последствия их воздействия и достигнутый уровень БИ в результате ее защиты.

Сейчас отсутствуют модели, позволяющие оценивать эффективность защиты информации (ЗИ) по размеру ущерба (предотвращенного ущерба).

При построении ущербно-затратной (стоимостной) модели безопасной системы основной задачей является выбор показателей эффективности мер ЗИ. Для выбора показателей эффективности предполагается ввести классификацию видов последствий воздействия угроз (ущерба от нарушения БИ) (рис. 1). Здесь под ущербом подразумевается

Рис.1. Основные показатели ущерба от нарушения БИ в ЛВС: ТТХ – тактико-технические характеристики; ПС – программные средства

размер предотвращенного ущерба, т.е. те средства, которые необходимо затратить на восстановление первоначального состояния аппаратных и программных составляющих локально-вычислительной сети (ЛВС).

Далее необходимо привести классификацию затрат на реализацию СЗИ (рис.2).

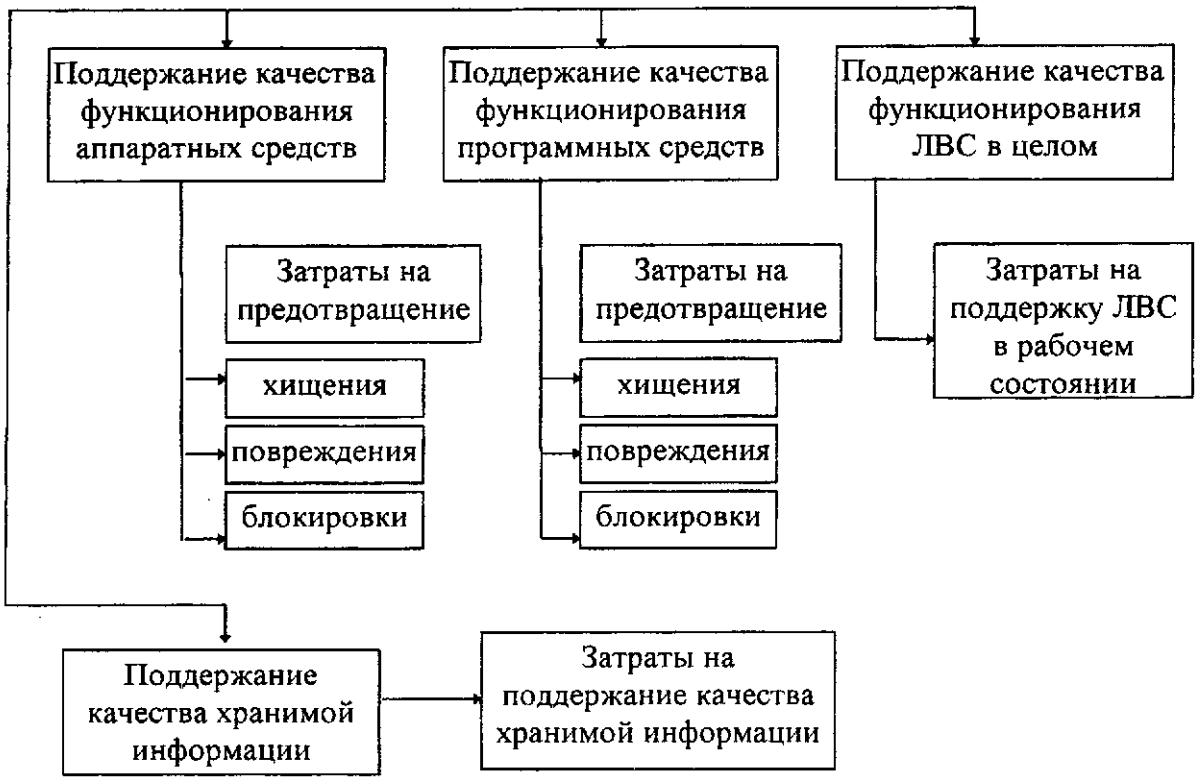

Рис. 2. Классификация затрат на реализацию СЗИ

Целесообразно применить стандартный экономический подход к оценке любых материальных проектов, спроецировав его на проблемы обеспечения БИ, т.е. на соотношение «ущерб от нарушения БИ – стоимость СЗИ» (рис.3).

По соотношению затрат на СЗИ и размера потенциального ущерба можно делать выводы об эффективности системы защиты организации. Области риска введены для учета фактора жесткости политики безопасности различных организаций, работающих с ЛВС. В основе этого лежит критерий оптимальности выбора средств защиты.

Приведем математическое описание изложенной модели.

В основе модели лежит критерий оптимальности выбора средств защиты:

$$\Sigma C_{\text{АПП}} + \Sigma C_{\text{ПР}} + \Sigma C_{\text{ЛВС}} + \Sigma C_{\text{ИНФ}} = \Sigma D_{\text{АПП}} + \Sigma D_{\text{ПР}} + \Sigma D^{1}_{\text{ЛВС}} + \Sigma D^{2}_{\text{ЛВС}} + \Sigma D_{\text{ИНФ}}$$

или

$$\sum_{k} C = \sum_{n} D,$$

где C – множество видов затрат на реализацию СЗИ; D – множество видов ущерба от проявления угроз БИ; k – размер множества затрат на СЗИ; n – размер множества видов ущерба.

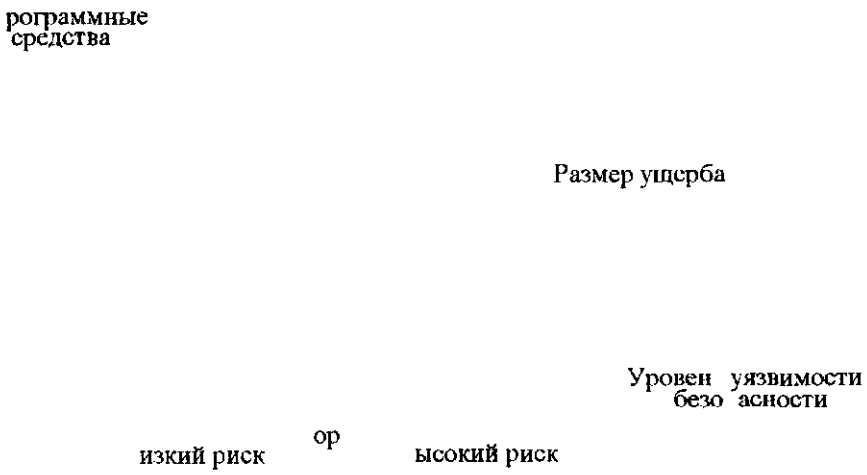

Рис Ущербно затратная модель обеспечения И в ЛВС

ив анноз и ие жно вы о ня ься ля ЛВС с оптимальной сте енью иска.

внутреннего пользования», «Персональная информация», «Коммерческая тайна», «Критическая информация».

• *Объемы хранящейся в ЛВС информации* – синтаксический показатель, принимающий значения: «Минимальный набор данных», «База данных масштаба небольшого предприятия», «База данных масштаба крупного предприятия», «База данных масштаба правительственных учреждений».

• *Количество задач, решаемых с помощью ЛВС* – численный показатель, определяющий среднее число действующих проектов, использующих ресурсы ЛВС.

• *Размер потенциального ущерба от выхода ЛВС из строя* – синтаксический показатель, принимающий значения: «Незначительный ущерб», «Ущерб, сопоставимый с недельной прибылью», «Ущерб, сопоставимый с месячной прибылью», «Ущерб, ставящий под угрозу существование организации».

• *Реакция клиентов на снижение качества функционирования ЛВС* – синтаксический показатель, принимающий значения: «Незначительная», «Недовольство», «Отток части клиентов», «Полный разрыв отношений с невозможностью будущего восстановления».

• *Жесткость политики безопасности ЛВС* – синтаксический показатель, принимающий значения: «Практическое отсутствие контроля безопасности», «Формальный контроль основных угроз», «Контроль недопущения воздействия большинства угроз», «Четкий контроль большинства угроз с требованием неукоснительного соблюдения всеми служащими», «Всеобъемлющий контроль всех возможных угроз с наказанием за несоблюдение».

Абсолютную степень риска определим как

$$R_{\text{АБС}} = \frac{\sum_{i=1}^{m} R_i \; P_i}{m},$$

где R_i – количественный показатель каждого отдельно взятого фактора; P_i – вес фактора; m – число влияющих факторов (в данном случае 6). В случае синтаксических переменных необходимо лингвистические значения перевести в относительные численные, которые варьируются в пределах $-N...N$, где $-N$ соответствует наиболее низкому значению синтаксического показателя, а N – наиболее высокому. Показатель N определяется в зависимости от выбранной системы взвешивания факторов и не является существенным параметром. Он влияет лишь на определение окрестности нуля при последующей классификации степени риска. Так, например, при $N = 10$ для показателя «Важность обрабатываемой информации» наиболее высокому значению синтаксической переменной («Критическая информация») будет соответствовать количественное значение R_i, равное 10, наиболее низкому («Для внутреннего пользования») – значение –10, промежуточным значениям – соответственно –3,3 и 3,3. Остальные показатели определяются точно так же. Полученное значение $R_{\text{АБС}}$ определяет степень риска организации следующим образом:

степень риска:	оптимальная	– при $R_{\text{АБС}} \to 0$;
	высокая	– при $R_{\text{АБС}} > 0$;
	низкая	– при $R_{\text{АБС}} < 0$.

Применение затратно-ущербной модели сопряжено с трудностями оценки стоимостного выражения предотвращенного ущерба и средств, затрачиваемых на применение защитных мероприятий. Однако даже пробная оценка при условии правильного определения степени риска позволяет выявить оптимальный перечень применяемых защитных механизмов в зависимости от размера потенциального ущерба. Модель позволяет концептуально определить стратегию защиты и оптимальный с экономической точки зрения набор средств защиты. В завершение приведен практический метод определения степени риска безопасной локальной сети.

Стаття надійшла до редакції 27 вересня 1999 року.