УДК 519.85

ОЦЕНКА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПО КРИТЕРИЮ «ЭФФЕКТИВНОСТЬ – СТОИМОСТЬ»

д.ф.-м.н., проф. М.В. Новожилова, К.А. Овечко

В статье рассматриваются основные тенденции в области информационной безопасности, предлагается модель оценки эффективности и стоимости проектируемой системы защиты информации (СЗИ).

Постановка проблемы. Компьютерные информационные системы являются неотъемлемой частью любого предприятия, причем их эффективность в первую очередь зависит от сохранности передаваемой и хранимой в них информации [1, 2]. Защита коммерческой информации является очень дорогой. Отсутствие этой защиты или недостаточно высокий уровень могут привести к серьезному нарушению прав и интересов предприятия с катастрофическими последствиями [2, 3]. Таким образом, появляется необходимость оценки информационной безопасности конкретного предприятия, определения возможных угроз по нарушению этой безопасности, вероятности того, что конкретная угроза реализуется на протяжении определенного периода времени, определения последствий реализации этих угроз.

Анализ последних публикаций. В силу того, что данная область является достаточно широкой, большая часть литературы посвящена рассмотрению определенных аспектов, или является обобщающей, не затрагивающей принципов реализации конкретных средств защиты.

Для проведения оценки качества работы проектируемой системы защиты информации (СЗИ) в работах [2, 3] анализируется несколько методик, в том числе методика оценок фирмы IBM, методика экспертных оценок. Одним из наиболее удачных на взгляд авторов является критерий «эффективность-стоимость», использование которого позволяет учесть наиболее важные характеристики СЗИ, являющиеся критичными при выборе средств защиты информации.

Математическая модель оценки СЗИ. Для оценки реакции информационной системы на изменения внешних и внутренних факторов использовался следующий подход. Во-первых, само предприятие характеризовалось такими основными показателями как доход, грн., количе-

ство рабочих мест, шт.

Далее выделялись информационные риски, угрожающие выбранному конкретному предприятию. Для каждого из рисков можно определить такие показатели, как вероятность осуществления данного риска; абсолютный ущерб, наносимый риском, в гривнях (размер ущерба не зависит от дохода предприятия); относительный ущерб, наносимый риском (исчисляется в процентах от дохода предприятия).

Ущерб при осуществлении угрозы для предприятия рассчитывается как:

$$У_r = A_r + Д \times O_r / 100,$$

где Уr – ущерб от r-й угрозы, грн.; Ar – абсолютный ущерб, наносимый предприятию r-й угрозой, грн.; Or – относительный ущерб, наносимый предприятию r-й угрозой, %; Д – доход предприятия, грн; r – номер угрозы/риска; r = 1, 2, … , R; R – количество рассматриваемых для данного предприятия рисков.

Для получения значения ожидаемого ущерба по r-у риску необходимо умножить величину ущерба $У_r$ на вероятность осуществления риска

$$ОУ_r = У_r \times P_r,$$

где ОУr – ожидаемый ущерб от r-го риска (степень риска), грн.; P_r – вероятность осуществления r-го риска.

Подсчет суммарного ожидаемого ущерба $ОУ^{сум}$, наносимого предприятию рисками, осуществляется по формуле:

$$ОУ^{сум} = \sum_{r=1}^{R} (A_r + O_r \times Д / 100) \times P_r .$$

Для уменьшения значения ожидаемого суммарного ущерба предприятие вынуждено расходовать часть своих средств на покупку, внедрение и эксплуатацию средств защиты информации. Для средств защиты можно выделить такие основные характеристики, как постоянные затраты, грн.; переменные затраты, грн. / рабочее место.

Постоянные затраты не зависят от размеров предприятия, численности рабочего персонала, объемов обрабатываемой и используемой предприятием информации. Переменные затраты зависят от перечисленных параметров, поэтому, для данных целей и была внедрена такая характеристика предприятия, как количество рабочих мест. Данный параметр является обобщающим и усредненным значением, призванным выполнить корректировку объема затрачиваемых денежных средств на внедрение средств защиты информации для различных предприятий.

Для выбранных средств защиты суммарные денежные расходы на

построение СЗИ $С_{СЗИ}$ определяются по следующей формуле:

$$С^{СЗИ} \sum_{s=1}^{S} З_s^{пос} + З_s^{пер} \times М,$$

где s – номер средства защиты, s = 1, 2, …, S; S – количество средств в СЗИ; $Зs^{пос}$ – постоянные затраты по внедрению и использованию s-го средства защиты, грн.; $Зs^{пер}$ – переменные затраты по внедрению и использованию s-го средства защиты, грн./рабочее место; М – количество рабочих мест на предприятии, шт.

Каждое из средств защиты обладает набором методов, позволяющих снизить ущерб, наносимый рисками. Для методов защиты выделяются следующие параметры:

– снижение вероятности осуществления риска (в процентах от вероятности осуществления риска);

– снижение значения абсолютных потерь (в процентах от абсолютных потерь, наносимых риском);

– снижение значения относительных потерь (в процентах от относительных потерь, наносимых риском).

Сумма сохраненных средств $МС_{sr}$ рассчитывается по формуле:

$$МС_{sr} = (А_г + Д \times О_г / 100) \times Р_г - (100 - Р_{sr}^{сн}) \times Р_{sr} \times [А_г \times (100 - А_{sr}^{сн}) / 100 + Д \times О_г \times (100 - О_{sr}^{сн}) / 10^4] / 100,$$

где $Аsr^{сн}$ – понижение значения абсолютного ущерба, наносимого предприятию r-м риском благодаря s-му средству; $Оsr^{сн}$ – понижение значения относительного ущерба, наносимого предприятию r-м риском благодаря s-му средству; $Рsr^{сн}$ – понижение вероятности осуществления r-го риска благодаря s-му средству.

В случае, если несколько средств защиты содержат методы борьбы против одного риска, то в СЗИ учитывается только наиболее эффективное средство. Таким образом, оценка суммарного объема средств $С^{сум}$, которые могут быть сохранены проектируемой СЗИ, определяется по формуле

$$С^{сум} = \sum_{s=1}^{S} \max_{r} МС_{sr} .$$

В таком случае сумма ожидаемого возможного ущерба ОВУ представляет собой разницу между ожидаемым суммарным ущербом $ОУ^{сум}$, наносимым рисками предприятию, и суммой всех средств $С^{сум}$, сохраненных СЗИ от рисков:

$$ОВУ = ОУ^{сум} - С^{сум} .$$

Суммарные затраты предприятия, связанные с информационной безопасностью, в этом случае состоят из расходов на покрытие возможного ущерба и расходов на построение СЗИ:

$$З^{сум} = ОВУ + С^{СЗИ},$$

где $З^{сум}$ – суммарные расходы предприятия, связанные с информационной безопасностью, грн.

Таким образом, критерий «эффективность-стоимость» выражен показателем $З^{сум}$, где эффективность СЗИ учитывается в виде составляющей ОВУ (чем меньше ОВУ, тем выше эффективность), а стоимость представлена $С^{СЗИ}$.

Выводы. Представленная математическая модель описывает основные наиболее существенные свойства исследуемой ИС и может служить основой для компьютерного моделирования системы средств защиты информации. При разработке программного продукта особое внимание следует уделить созданию и обновлению базы данных по существующим средствам защиты информации.

ЛИТЕРАТУРА

1. *Мелл П., Фэррейело Д. Обеспечение безопасности WEB-серверов // Конфидент. – 2001. – № 1. – С. 23 – 25.*
2. *Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: DiaSoft, 1999. – 480 с.*
3. *Домарев В.В. Безопасность информационных технологий. – К.: DiaSoft, 2002. – 672 с.*

Поступила 28.10.2003

НОВОЖИЛОВА Мария Владимировна, *д.ф.-м.н., проф., зав. кафедрой компьютерного моделирования и информационных технологий ХГТУСА. Окончила ХИРЭ в 1984 году. Область научных интересов – математическое и компьютерное моделирование сложных систем.*

ОВЕЧКО Константин Александрович, *аспирант Харьковского государственного технического университета строительства и архитектуры, который окончил в 2003 году. Область научных интересов – автоматизированное проектирование трудноформализуемых систем.*