симости, характеризующие степень влияния внутренних угроз на безопасность информации ограниченного распространения.

Результаты моделирования показывают, что уже после второго шага система может оказаться в поглощающем состоянии, соответствующего реализации злоумышленником внутренней угрозы

Увеличение числа шагов процесса перехода системы из состояния в состояние не только увеличивает его длительность, но и число особых ситуаций, возникающих в результате воздействия на систему внутренних угроз, а, следовательно, и к росту вероятности оказаться в поглощающем, неблагополучном состоянии.

Собственник информации ограниченного распространения может использовать полученные количественные зависимости для разработки научно-обоснованных мероприятий по применению защитных механизмов в зависимости от имеющихся методов и средств, а также располагаемых материальных ресурсов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Тихонов, В.И., Миронов, М.А.* Марковские процессы. – М.: Советское радио,1997. – 488 с.

2. *Вентцель, С. Е*. Исследование операций. – М.: Советское радио,1972. – 550 с.

3. *Росенко, А.П.* Марковские модели оценки безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему внутренних угроз[Текст] / Росенко А.П. // Вестник Ставропольского государственного университета. – Ставрополь: СГУ, 2005. – С. 34-40.

4. *Росенко, А.П.* Научно-теоретические основы исследования влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированных информационных системах [Текс] / Росенко А.П. // Известия ТРТУ. Материалы VII международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2005. – С. 19-30.

5. Внутренние ИТ-угрозы в России 2006. www.infowatch.ru.

6. *Росенко, А.П., Клименко, Е.С.* О выборе критерия оценки эффективности функционирования системы защиты информации [Текст]/ Росенко А.П., Клименко Е.С. // Первая международная научно-техническая конференция. Инфотелекоммуникационные технологии в науке, производстве и образовании. – Ставрополь: Изд-во Сев-Кав. ГТУ, 2004. – С. 207-208.

УДК 683.34

Ю.К. Язов, Т.В. Григорьева

ПАРАДИГМА ПРЕДЕЛЬНОГО УЩЕРБА И ЕЕ ИСПОЛЬЗОВАНИЕ ПРИ ОЦЕНКЕ РИСКОВ НАРУШЕНИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ

В данной статье рассматривается один из важных и актуальных вопросов развития методологии количественной оценки эффективности защиты информации – построение шкал комплексной оценки рисков нарушений безопасности информации на основе парадигмы предельного ущерба. Указанная парадигма широко используется в жизни при различных видах оценок. Ее суть заключается в установлении верхней границы шкалы оценок, выше которой значение оцениваемого параметра не влияет на выводы относительно объекта оценки (оцениваемого процесса, явления, события, уровня знаний и т.п.) и, в частности, относительно риска нарушения безопасности информации в компьютерной системе, определяемого,

прежде всего, размерами возможного ущерба от реализации угроз безопасности информации. Это позволяет построить так называемые оппозиционные (полярные) шкалы, основанные на установлении, по крайней мере, двух противоположных (в этом смысле полярных) точек на шкале, определяющих крайние противоположные результаты оценки ущерба (отсутствие ущерба и неприемлемый ущерб).

Ущерб от реализации угрозы безопасности информации определяется содержанием несанкционированного действия, выполняемого в ходе реализации угрозы относительно защищаемой информации, системного или прикладного программного обеспечения, и является в общем случае величиной случайной. Поэтому, как правило, проводится оценка среднего значения ущерба. В [1] было показано, что для оценки величины ущерба может быть использовано отношение средней величины ущерба от выполнения несанкционированного действия в случае реализации угрозы к предельно допустимой величине ущерба (неприемлемому ущербу), которое названо индексом ущерба:

$$\beta_u = \frac{\bar{u}}{u_{\lim}}. \qquad (1)$$

Если имеется числовая шкала и на ней определена величина предельного ущерба, то индекс ущерба рассчитывается по приведенной формуле. Однако, если числовую шкалу ущербов построить не удается, то строится вербальная, то есть шкала нечетких суждений, на которой определяется точка предельного ущерба и все ущербы выше этой точки рассматриваются как недопустимые.

На основе индекса ущерба может быть введена функция, с помощью которой может быть оценена опасность как каждого несанкционированного действия, так и совокупности таких действий, которые могут иметь место относительно защищаемого блока информации при реализации множества угроз безопасности информации. Такая функция названа коэффициентом опасности.

Если выполняется только одно $g-$е несанкционированное действие, то коэффициент опасности этого действия определяется следующим образом:

$$K_g = \begin{cases} \beta_g, \ \textit{если} \ \ \beta_g \le 1; \\ 1, \ \ \textit{если} \ \ \beta_g > 1 \ . \end{cases} \qquad (2)$$

При этом $K_g \le 1$ определяется на нормированной полярной шкале оценок.

Если ущерб оценивается по нечеткой шкале, то необходимо найти нечеткие отношения между индексом ущерба и содержанием нарушения безопасности рассматриваемого блока информации. В основе построения таких отношений лежит исходное положение о том, что всегда можно составить ряд предпочтения для возможных последствий от нарушений безопасности информации. Это позволяет определить весовые коэффициенты для каждого последствия нарушений. В случае отсутствия каких-либо оснований (сведений) для выявления весового коэффициента можно использовать известное правило Фишберна [2], в соответствии с которым, если на множестве рассматриваемых характеристик (в данном случае последствий от нарушений безопасности рассматриваемого блока информации), количество которых равно N, установлены отношения предпочтения $r_1 \ge r_2 \ge ... \ge r_N$, то значимость n-го последствия определяется из соотношения:

$$r_n = \frac{2 \cdot [N - n + 1]}{[N + 1] \cdot N}, \quad (3)$$

что соответствует максимуму неопределенности сведений о компьютерной системе [2].

Введенная таким образом система весовых коэффициентов на всем множестве последствий реализации угроз безопасности информации позволяет построить простую шкалу оценок опасности последствий следующим образом:

$$\beta_n = \frac{r_n}{\max\limits_{n \in N}(r_n)} = 1 - \frac{n-1}{N}. \quad (4)$$

Особенность такой шкалы заключается, прежде всего, в ее универсальности относительно видов ущерба. Учет этой особенности важен при оценке опасности совокупности угроз, реализация которых может привести к разнородным ущербам: финансовому, материальному, моральному, ущербу здоровью граждан и др.

Кроме того, оценка по таким шкалам является условной, поскольку верхняя граница шкалы обусловлена суждением о неприемлемости ущерба для данного конкретного обладателя информации. Такая условность очень характерна для объектов информатизации, поскольку для разных объектов информатизации один и тот же ущерб может оцениваться по-разному.

Предельный ущерб отражает представление обладателя информации о ее важности. Однако нарушение безопасности защищаемой в данной компьютерной системе может затрагивать интересы не только организации, которой принадлежит данная система, но и интересы региона или даже государства в целом, что необходимо учитывать при оценке опасности угроз. При этом, если для данного предприятия или организации нарушение безопасности защищаемой информации может привести к неприемлемому ущербу, то в рамках региона этот ущерб может оказаться незначительным и тем более незаметным в рамках государства.

Для учета и парирования такой условности в оценке ущерба может быть использован метод взаимосвязанных шкал с их перенормировкой при переходе от одной шкалы к другой. Суть метода сводится к следующему.

Во-первых, для учета уровня инстанции, чьи интересы затрагиваются при нарушении безопасности информации в данной компьютерной системе, вводятся L уровней (градаций) важности, при этом первый уровень соответствует наибольшей, а последний – наименьшей важности. Пример вербальной интерпретации каждого уровня приведен в табл.1.

Для каждого l-го уровня важности строится своя шкала оценок величины возможного ущерба, по которой оценивается коэффициент опасности.

Во-вторых, для каждой шкалы вводится относительный коэффициент ее важности $\alpha(l, m)$, лежащий в пределах от 0 до 1, следующим образом:

$$\alpha(m,l) = f(m,l), l = \overline{1,m},\ m = \overline{1,L}, \quad (5)$$

где $f(m,l)$ – некоторая (линейная или нелинейная) функция.

Примеры такой функции приведены в табл.2.

Таблица 1

Пример вербальной интерпретации уровней важности защищаемой информации при оценке возможных ущербов

Наименование уровня важности	Номер уровня важности	Краткая характеристика уровня
Федеральный (государственный)	1	Затрагиваются интересы государства, министерств, первых лиц государства. Возможно развитие федеральной чрезвычайной ситуации
Региональный	2	Затрагиваются интересы региона. Возможно развитие региональной чрезвычайной ситуации с охватом территории не менее двух субъектов федерации
Территориальный	3	Затрагиваются интересы субъекта федерации. Возможно развитие территориальной чрезвычайной ситуации
Местный	4	Затрагиваются интересы города, района, населенного пункта. Возможно развитие местной чрезвычайной ситуации
Объектовый, корпоративный	5	Затрагиваются интересы предприятия, организации, фирмы. Возможно развитие объектовой чрезвычайной ситуации
Групповой	6	Затрагиваются интересы подразделения (нескольких подразделений) организации, предприятия, первых лиц организации (предприятия).
Персональный (пользовательский)	7	Затрагиваются интересы пользователя (нескольких пользователей)

Таблица 2

Примеры функции, определяющей относительный коэффициент важности шкалы оценок ущерба

Наименование зависимости	Вид функции	Примечания
Линейная	$\alpha(m,l)=\alpha_{\min}+\frac{1-\alpha_{\min}}{L-l+1}\cdot(L-m+1)$	L – общее количество уровней важности; $\alpha_{\min}$ – относительный коэффициент важности (отношение самого низкого к самому высокому уровню важности); l – номер уровня важности, относительно которого пересчитывается коэффициент опасности для уровня m

Окончание табл. 2

Наименование зависимости	Вид функции	Примечания
Квадратичная	$\alpha(m,l) = a \cdot m^2 + b \cdot m + c,$ $a = \frac{(1-\alpha_{\min})}{(L-l)^2};\ b = 2 \cdot \frac{(1-\alpha_{\min})}{(L-l)^2} \cdot L;$ $c = \alpha_{\min} + (1-\alpha_{\min}) \frac{L^2}{(L-l)^2}$	a, b, c – параметры параболы, при условии, что $l < L, m \le l$
Степенная	$\alpha(m,l) = (\frac{L-m+1}{L-l+1})^n,$ $n = \frac{1}{L-l+1} \cdot \ln(\frac{1}{\alpha_{\min}})$	
Показательная	$\alpha(m,l) = c \cdot e^{b \cdot m},$ $b = \frac{\alpha_{\min}}{L-l};\quad c = e^{-\frac{\alpha_{\min} \cdot l}{L-l}}$	b, c – параметры показательной функции, при условии, что $l < L, m \le l$

С использованием относительных коэффициентов важности шкала с уровнем меньшей важности может быть нормирована относительно шкалы с уровнем большей важности, то есть оценка коэффициента опасности $K_g^{(m)}$ по шкале с уровнем важности m может быть пересчитана на значение данного коэффициента $K_g^{(l)}$ по шкале с уровнем важности l, при этом:

$$K_g^{(l)} = \alpha(m,l) \cdot K_g^{(m)}. \qquad (6)$$

Приведенные соотношения позволяют нормировать шкалы, построенные на нижнем уровне важности, относительно шкал с более высоким уровнем важности и тем самым парировать условность введения предельно допустимого уровня ущерба.

Пример построения подобных шкал и возможность их сведения к единой универсальной шкале оценок возможных ущербов показан на рис.1.

Достоинствами предложенного подхода являются:

- инвариантность к видам шкал, по которым оцениваются парциальные ущербы от реализации разнородных угроз безопасности информации;
- возможность приведения принципиально разнородных шкал к единой шкале оценок;
- возможность применения нечетких оценок возможного ущерба от реализации угроз безопасности информации;
- парирование сложности учета разных оценок одного и того же ущерба разными пользователями за счет введения операции нормирования по условному предельно допустимому ущербу.

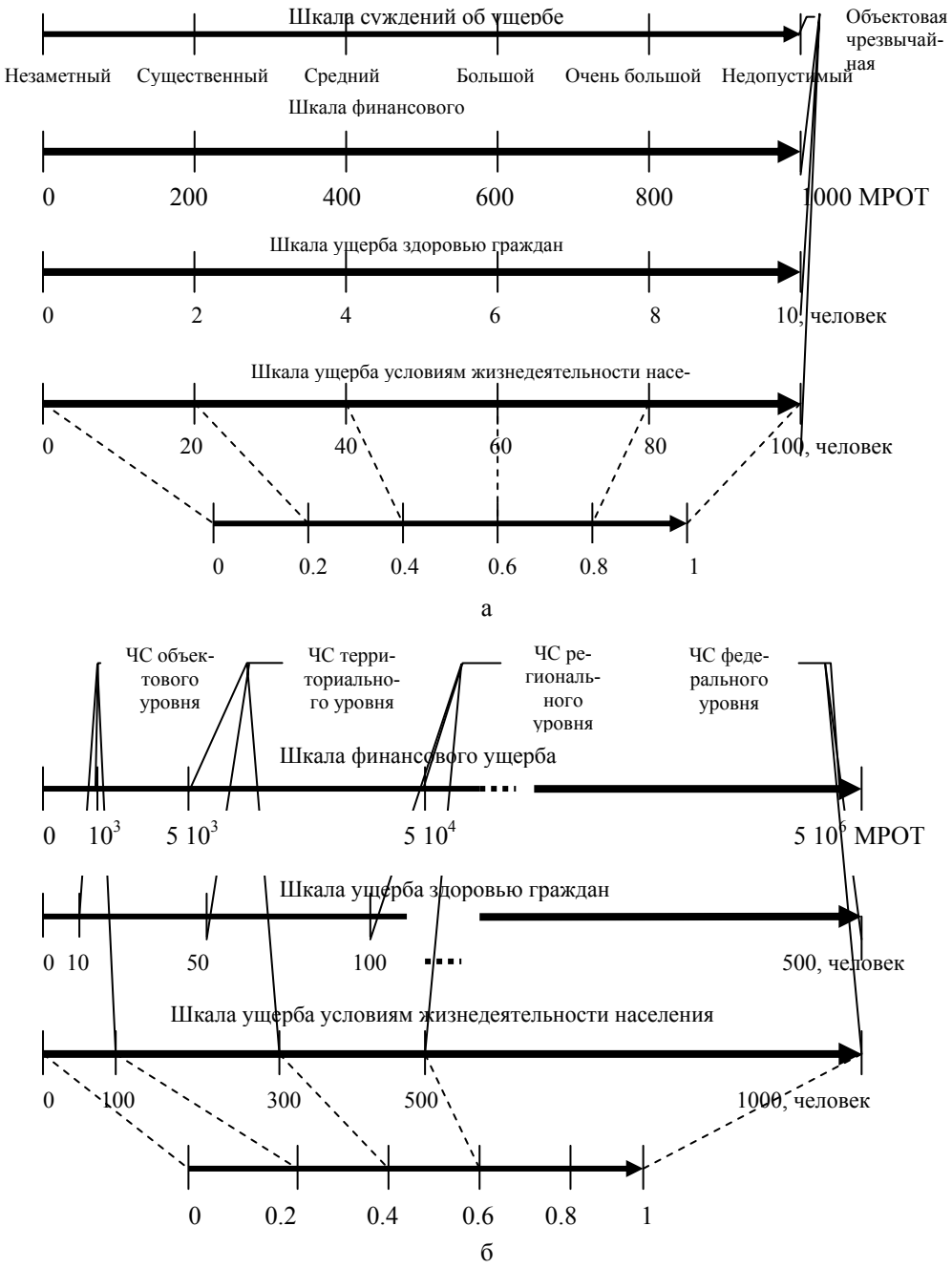

Рис.1. Примеры шкал оценок ущерба от реализации угроз безопасности информации в компьютерных системах: а – относительно ущерба, соответствующего чрезвычайным ситуациям объектового уровня; б – относительно ущерба, соответствующего чрезвычайным ситуациям федерального уровня

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Язов Ю.К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 274 с.
2. *Fishburn P.* Utility Theory for Decision-Making. N.Y., Wiley, 1970.

УДК 004.056

В.В. Золотарев

МЕТОД ИССЛЕДОВАНИЯ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОМПОНЕНТНОЙ МОДЕЛИ ОПЕРАЦИОННОЙ СРЕДЫ*

Введение

Представлены результаты, обобщающие процедуру анализа внутренних характеристик средств защиты и их влияния на операционную среду. Основой подхода является выделение внутренних критериев оценки взаимодействий и оценка внутренних структур.

Особенности программного обеспечения и программно-аппаратных комплексов, применяемых для решения задач защиты информации, часто позволяют нарушать безопасность защищаемого объекта или снижать его уровень защищенности. Механизмы такого влияния связаны с реализацией средств защиты информации (СЗИ), а также с взаимным влиянием внутренних параметров СЗИ и операционной среды. Рассматривая практические подходы к такому анализу, можно отметить несколько недостатков, не позволяющих в общем случае провести полный анализ защищенности:

– использование методов анализа, базирующихся на оценке множества известных угроз и уязвимостей, не позволяющих сделать корректный прогноз существования неизвестных;

– неформализованный подход к решению большинства задач, и, как следствие, математически не доказанные факты взаимного влияния внутренних параметров СЗИ и операционной среды;

– неполные или некорректные методы извлечения информации о взаимодействии СЗИ и операционной среды, приводящие к неполным или искаженным выводам по результатам исследования.

Таким образом, постановка задачи в работе следующая: требуется сформулировать, алгоритмизировать и предварительно оценить метод исследования взаимного влияния внутренних параметров СЗИ и операционной среды.

Можно рассмотреть как единый метод исследования, так и частные методы. Далее в статье рассмотрен единый метод, который, в свою очередь, имеет дальнейшее развитие в область частных оценок.

Общая характеристика области исследования

Внутренние параметры средства защиты информации и операционной среды представляют собой в рамках исследования строго не определенную область, которая может быть расширена и/или детализирована. Безусловно, к параметрам средств защиты информации необходимо вне зависимости от поставленной задачи относить следующий набор характеристик:

* Работа выполнена при поддержке гранта Президента МК-3625.2007.9.