В. К. Джоган, А. П. Курило

ЗАЩИЩЕННОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЬЮТЕРНЫХ СИСТЕМ КАК СИСТЕМА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Системность решения актуальной проблемы обеспечения информационной безопасности компьютерных систем достигается всесторонним анализом существующих подходов к обеспечению защиты компьютерной информации. Взаимосвязанная совокупность методов и средств, реализующих эти подходы, представляет собой механизм обеспечения защищенности информации этих систем. То обстоятельство, что компьютерные системы характеризуются множеством нетривиальных свойств, относит вопросы их исследования к числу сложных как в научном, так и в практическом плане.

Исследование механизмов обеспечения защищенности информационных ресурсов компьютерных систем предполагает:

- проведение системного анализа состояния информационной безопасности системы в целом и отдельных ее сегментов;
- исследование путей построения исследуемых механизмов;
- оценку защищенности информационных ресурсов.

Наиболее сложной из перечисленных проблем является проблема оценки качества защиты компьютерной информации. Сложность и отсутствие очевидного решения этой проблемы и, как следствие, недостаточный уровень научно обоснованных рекомендаций при оценке защищенности информационных ресурсов компьютерных систем являются причинами множества допускаемых методических ошибок в процессе выявления и предупреждения угроз их безопасности.

Анализ существа проблемы оценки защищенности информационных ресурсов компьютерных систем позволил выделить ряд взаимосвязанных аспектов. Во-первых, в общем случае отсутствуют формальные методы объективного обоснования набора оценочных показателей и требований к их значениям. Очевидно, это обусловлено как многообразием характеристик защищенности информации, связанным со сложностью, размерами и организационно-технической природой компьютерных систем, так и с широким диапазоном и динамикой пользовательских требований.

Это обусловило необходимость поиска таких подходов к исследованию механизмов обеспечения защищенности информационных ресурсов компьютерных систем, которые системно учитывали бы все множество свойств входящих в состав этих механизмов компонентов.

Как показывает анализ состояния проблемы исследования механизмов обеспечения защищенности информационных ресурсов компьютерных систем, одним из наиболее перспективных путей ее решения является обобщение отдельных частных показателей эффективности этих механизмов. Вместе с тем процесс обобщения этих показателей имеет ряд особенностей, обусловленных априорной неопределенностью их взаимосвязей для адекватной характеристики возможностей исследуемых механизмов.

В данной статье рассматривается методический подход к решению проблемы оценки защищенности информационных ресурсов компьютерных систем, суть которого состоит в установлении научно обоснованных правил синтеза системы частных показателей эффективности механизмов обеспечения защищенности.

В отличие от материалов, представленных в более ранних публикациях авторов по данной проблеме, где в качестве классификационного основания при построении системы показателей выбирался один доминирующий параметр: информационный объем [1] или время обработки

информации [2], в данной статье рассматривается возможность варьирования этими параметрами как классификационными основаниями для определения всех основных показателей защищенности информации в компьютерных системах.

Выбрав в качестве классификационного основания способ измерения характеристик защищенности информационных процессов в компьютерных системах, выделим множество объективных и субъективных показателей защиты информации в этих системах [1–4].

Объективные показатели позволяют измерять и оценивать по шкале отношений качество защиты информации в компьютерных системах с технологической точки зрения. К объективным показателям качества защиты информации в компьютерных системах относятся:

1. Объем защищаемой информации ($e_1^{(o)}$), характеризующий потребности в обеспечении установленного статуса ее хранения, обработки и использования;

2. Время выполнения процедуры защиты ($e_2^{(o)}$), характеризующее временной интервал с момента начала действий, предпринятых для выполнения процедуры защиты информации, до момента их завершения.

Измерение и оценка субъективного качества защиты информации в компьютерных системах производятся на основе субъективных показателей непосредственно пользователем.

Основными субъективными показателями качества защиты информации в компьютерных системах являются:

1. Степень проявления (воздействия) угрозы информационной безопасности — $e_1^{(c)}$. Существует целый ряд моделей угроз информационной безопасности компьютерных систем, позволяющих определить данный показатель. Наиболее известными из этих моделей являются модели надежности информационной системы, с помощью которых определяются вероятностные характеристики воздействия угроз нарушения целостности и доступности информации [5], и модели нарушителя [6], позволяющие определить вероятностные характеристики угроз нарушения конфиденциальности (утечки) информации.

2. Конфиденциальность информации ($e_2^{(c)}$), характеризующая требование, обязательное для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия ее обладателя [7].

3. Целостность информации ($e_3^{(c)}$), характеризующая способность обеспечивать предоставление права ее модификации (уничтожения) только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность в условиях случайных ошибок или стихийных бедствий [8].

4. Доступность информации ($e_4^{(c)}$), характеризующая свойство информационной технологии обеспечивать свободный доступ к информации по мере возникновения необходимости [8].

5. Своевременность реализации функций защиты информации ($e_5^{(c)}$), характеризующая время, в течение которого эти функции удовлетворяют предыдущие требования [2, 4].

Проведенное обоснование показателей качества защиты информации в компьютерных системах дает возможность понять механизмы их измерения и как инструмент оценки формально представить в виде множества:

$$E = \{e_i\},\ i = 1, 2, \ldots, |E|, \qquad (1)$$

в котором e_i определены на различных подмножествах объективных $\{e_1^{(o)}, e_2^{(o)}\}$ и субъективных $\{e_k^{(c)}\}$, $k = 1, 2, \ldots, 5$, показателей и имеют различную шкалу измерения.

Каждый из показателей качества, в свою очередь, представляет собой упорядоченное множество (непрерывное, дискретное или состоящее из переменных (0,1)):

$$e_i = \{э_{il}\},\ l = 1, 2, \ldots, L,\ э_{i1} < э_{i2} < \ldots < э_{iL}. \qquad (2)$$

Формально качество определяется через частично упорядоченное множество:

$$\tilde{E} = \{\tilde{e}_m\},\ \varphi: C\ Ч\ E \to \tilde{E}, \quad (3)$$

где φ — отображение прямого декартова произведения $C\ Ч\ E$ во множество $\tilde{E}$;

C — упорядочивающее множество.

Упорядочивающее множество C вносит отношение порядка в неупорядоченное множество показателей качества E защиты информации в компьютерных системах и формируется с использованием рангового порядка упорядочения показателей.

Структурированное представление качества защиты информации в компьютерных системах в виде (2) дает возможность его интегральной оценки. Такая оценка возможна с использованием векторного показателя $\vec{E}$, характеризующего защищенность информации и в семантическом и в технологическом плане:

$$\vec{E} = (e_1^{(o)}, e_2^{(o)}, e_1^{(c)}, e_2^{(c)}, \ldots, e_5^{(c)}), \quad (4)$$

где $e_j^{(o)}, e_k^{(c)}$ — соответственно скаляры объективных и субъективных показателей качества защиты информации в компьютерных системах.

Учитывая, что упорядочивающее множество C в (3) формируется с использованием рангового порядка упорядочения показателей в условиях систематизации показателей для интегральной оценки качества защиты информации в компьютерных системах, воспользуемся скаляризацией показателя (4) с учетом значений всех рассмотренных выше показателей. Процедура скаляризации реализуется следующим образом.

1. Все показатели защищенности информации делятся по критерию важности (рангам) для выполнения целевой функции на три категории: определяющие, существенные и второстепенные.

2. Требуемый уровень защиты информации устанавливается по значениям определяющих показателей защищенности информации.

3. Выбранный уровень в некоторых случаях может быть скорректирован с учетом степени значимости показателя (определяющая, существенная, второстепенная).

Поскольку конфиденциальность, целостность и доступность информации являются ее основными состояниями, значимость их показателей объективно носит определяющий характер.

Определив формально эти показатели через частично упорядоченные множества (вида (3)) скаляров вектора (4), интегральный показатель защищенности информационных ресурсов представим в виде:

$$\vec{E} = \langle \tilde{E}_{(к)}, \tilde{E}_{(ц)}, \tilde{E}_{(д)} \rangle, \quad (5)$$

где $\tilde{E}_{(к)} = e_2^{(c)}, \tilde{E}_{(ц)} = e_3^{(c)}, \tilde{E}_{(д)} = e_4^{(c)}$.

В этих условиях формальное представление уровня качества защиты информационных ресурсов компьютерных систем целесообразно осуществить с помощью лингвистических переменных (таблица 1).

Таблица 1. Классификация показателей качества защиты информации

№ п/п	Обозначение	Наименование показателя	Значимость показателя		
			Конфиденциальность, $e_2^{(c)}$	Целостность, $e_3^{(c)}$	Доступность, $e_4^{(c)}$
1	$e_1^{(c)}$	Степень проявления (воздействия) угрозы информационной безопасности	Существенная	Существенная	Существенная

2	$e_1^{(o)}$	Объем защищаемой информации	Существенная	Существенная	Второстепенная
3	$e_2^{(o)}$	Время выполнения процедуры защиты	Существенная	Второстепенная	Существенная
4	$e_5^{(c)}$	Своевременность реализации функций защиты информации	Существенная	Второстепенная	Существенная

С учетом изложенного рассмотрим варианты сочетания свойств объективного и субъективного качества показателей эффективности защиты информации компьютерных систем.

Возможности по защите информации от угроз нарушения ее конфиденциальности формально опишем условиями:

$$e_2^{(c)} = 1 \text{ при } \upsilon_{(n)} = 0 \quad (6)$$

и

$$0 \le e_2^{(c)} < 1 \text{ при } \upsilon_{(n)} > 0, \quad (7)$$

где $\upsilon_{(n)}$ — объем перехватываемой информации.

Будем полагать, что условие (6) является обязательным требованием к обеспечению конфиденциальности информации. В противном случае (условие (7)) конфиденциальность обеспечивается не в полном объеме.

В качестве доказательства функциональной зависимости показателя конфиденциальности информации от полноты ее объема оценим условно верхний уровень любого из рассмотренных показателей единицей. Тогда можно полагать, что

$e_1^{(o)} \to 1$, $e_2^{(o)} \to 0$, $e_1^{(c)} \to 0$, $e_j^{(c)} \to 1$, $j = 3, 4, 5$, при $e_2^{(c)} \to 1$.

Такие допущения позволяют производить оценку конфиденциальности информации в компьютерной системе посредством измерения необходимого объема защищенной от перехвата информации с учетом ее полноты, достоверности, целостности, доступности релевантности и своевременности.

С использованием аналогичных рассуждений возможности по защите информации от угроз нарушения ее целостности формально описываются условиями:

$$e_3^{(c)} = 1 \text{ при } e_1^{(o)} \ge \upsilon_{(д)} \quad (8)$$

и

$$e_3^{(c)} = 0 \text{ при } e_1^{(o)} < \upsilon_{(д)}, \quad (9)$$

где $\upsilon_{(д)}$ — минимально допустимый объем информации, при котором информация компьютерной системы считается целостной.

Будем полагать, что условие (8) является обязательным требованием к обеспечению целостности информации компьютерной системы. В противном случае (условие (9)) целостность информации нарушается.

В качестве доказательства функциональной зависимости показателя целостности информации от полноты ее объема оценим условно верхний уровень любого из рассмотренных показателей единицей. Тогда можно полагать, что

$e_1^{(o)} \to 1$, $e_2^{(o)} \to 0$, $e_1^{(c)} \to 0$, $e_j^{(c)} \to 1$, $j = 2, 4, 5$, при $e_3^{(c)} \to 1$.

Такие допущения позволяют производить оценку целостности информации компьютерных систем посредством измерения необходимого объема защищенной от искажения информации с учетом ее полноты, достоверности, конфиденциальности, доступности, релевантности и своевременности.

Анализ множества субъективных показателей качества защиты информации компьютерных систем дает основание утверждать, что характеристикой возможностей по защите информации от угроз нарушения ее доступности является показатель своевременности доступа.

Формально можно считать, что

$e_4^{(c)} = 1$ при $e_2^{(o)} \ \tau_{(д)}$ (10)

и

$e_4^{(c)} = 0$ при $e_2^{(o)} > \tau_{(д)}$, (11)

где $\tau_{(д)}$ — максимально допустимое время доступа к информации компьютерной системы.

Будем полагать, что условие (10) является обязательным требованием к обеспечению доступа к информации компьютерных систем. В противном случае (условие (11)) информация недоступна.

В качестве доказательства функциональной зависимости показателя доступности информации компьютерных систем от времени доступа оценим условно верхний уровень любого из рассмотренных показателей единицей. Тогда можно полагать, что

$e_1^{(o)} \to 1$, $e_2^{(o)} \to 0$, $e_1^{(c)} \to 0$, $e_j^{(c)} \to 1$, $j = 2, 3, 5$, при $e_4^{(c)} \to 1$.

Такие допущения позволяют производить оценку доступности информации в компьютерных системах посредством измерения необходимого времени реализации функций защиты информации от блокирования с учетом ее полноты, достоверности, конфиденциальности, целостности, релевантности и своевременности.

Смысловое сходство условий (6) с (8), (10) и (7) с (9), (11) дает возможность использовать в качестве основания для унификации описания соответствующих механизмов параметры этих условий. Кроме того, эти параметры дают количественное представление эффективности этих процессов [9].

Следует отметить, что в проблематике реализации информационных технологий и технологий защиты информации рассмотренные обстоятельства являются определяющими. Анализ условий (6)—(11) применительно к процессам обработки и защиты информации показал следующее:

1) минимально допустимый объем $\upsilon_{(п)}$, $\upsilon_{(д)}$ информации, удовлетворяющий потребности в обеспечении конфиденциальности и целостности информации, и максимально допустимое время доступа к информации в компьютерных системах $\tau_{(д)}$ определяются нормативными условиями защиты информации;

2) условия (6), (8), (10) являются обязательным требованием к реализации процедур обеспечения конфиденциальности, целостности и доступности соответственно;

3) в противном случае (условия (7), (9), (11)) реализация процедур защиты информации теряет всякий смысл;

4) показатели $e_2^{(c)}$, $e_3^{(c)}$ и $e_4^{(c)}$ носят вероятностный характер [9].

В совокупности указанные предпосылки создают основу формирования научно-методической базы для оценки качества защиты информации в компьютерных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. *Карпычев В. Ю., Курило А. П. [и др.]*. Проблема синтеза системы показателей для оценки качества защиты информации // Вопросы защиты информации. 2010. № 4 (91). С. 51—56.

2. *Карпычев В. Ю., Джоган В. К. [и др.]*. Своевременность как базовый показатель качества информационной деятельности в условиях противодействия угрозам безопасности // Информация и безопасность. Воронеж: Воронежский государственный технический университет, 2008. Вып. 4. С. 573—576.

3. *Скрыль С. В., Курило А. П. [и др.]*. Конфиденциальность как субъективный показатель защищенности информации // Безопасность информационных технологий. 2009. № 3. С. 141–144.
4. *Скрыль С. В., Багаев Д. А.* Своевременность как базовый показатель качества защиты информации // Вопросы защиты информации. 2009. № 2 (85). С. 61–63.
5. *Зарубин В. С., Киселев В. В. [и др.]*. О некоторых допущениях в математической интерпретации угроз нарушения целостности и доступности информации в компьютерных системах // Информация и безопасность. Воронеж: Воронежский государственный технический университет, 2009. Вып. 4. С. 625–626.
6. *Литвинов Д. В., Скрыль С. В., Тямкин А. В.* Исследование механизмов противодействия компьютерным преступлениям: организационно-правовые и криминалистические аспекты: монография. Воронеж: Воронежский институт МВД России, 2009. – 218 с.
7. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. 29 июля.
8. Основы информационной безопасности: учебник для высших учебных заведений МВД России / Под ред. В. А. Минаева и С. В. Скрыля. Воронеж: Воронежский институт МВД России, 2001. – 464 с.
9. Информационная безопасность и защита информации: сборник терминов и определений. М.: Гостехкомиссия России, 2001. – 149 с.
10. *Джоган В. К., Курило А. П. [и др.]*. Оценка защищенности информационных процессов в территориальных органах внутренних дел: модели исследования: монография. Воронеж: Воронежский институт МВД России, 2010. – 217 с.