А.А. Модестов, В.В. Степанов

МОДЕЛИРОВАНИЕ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ В КРИТИЧЕСКИ ВАЖНЫХ СЕГМЕНТАХ ИНФОРМАЦИОННОЙ СФЕРЫ

Первоочередными объектами противоправных действий криминальной среды являются информационные ресурсы так называемых критических инфраструктур, ущерб от нарушения информационной безопасности которых приводит к особо значительным, а подчас к фатальным последствиям.

К таким структурам относятся органы государственного управления, системы управления инфраструктурой связи, финансов, энергетики, транспорта, водоснабжения и чрезвычайных служб. Информационные элементы этих структур являются критически важными сегментами информационной сферы.

Отсюда все более актуальной становится проблема обеспечения безопасности критически важных сегментов информационной сферы. Очевидно, что ее решение должно осуществляться системно, на основе всестороннего исследования технологий обеспечения безопасности информационной сферы.

Взаимосвязанная и целеустремленная совокупность средств, реализующих эти технологии, представляет собой систему противодействия (СП) угрозам безопасности критически важным сегментам информационной сферы. То обстоятельство, что СП характеризуется множеством нетривиальных свойств, относит вопросы ее исследования к числу сложных как в научном, так и в практическом плане.

Все это обусловило необходимость поиска таких подходов в оценке эффективности СП, которые системно учитывали бы все множество свойств входящих в ее состав средств.

Как показывает анализ состояния проблемы, одним из наиболее перспективных путей решения данной задачи является построение математических моделей обобщения показателей, характеризующих возможности средств СП. Вместе с тем, процесс обобщения показателей имеет ряд особенностей, и, прежде всего, наличие нескольких степеней свободы в классификации возможностей средств СП. То же самое можно сказать и в отношении инструмента исследования средств СП - математических моделей процессов их функционирования.

Это позволило авторам предложить принципиально новый подход к решению задачи оценки возможностей СП по предотвращению ущерба информационной сфере от нарушения безопасности ее критически важных сегментов. Суть данного подхода состоит в разработке математических

моделей синтеза частных показателей в квазиоптимальную, с точки зрения оценки степени достижения целей СП, форму.

Для решения задачи совершенствования методов оценки противодействия угрозам безопасности в критически важных сегментах информационной сферы сформулирован ряд требований.

Основополагающим является ***требование поэтапной обобщаемости показателей эффективности СП***, в соответствии с которым структура показателей должна обеспечивать последовательное обобщение их групп до тех пор, пока в не сформируется единственный обобщенный показатель.

Из основополагающего вытекает ряд дополнительных требований.

Требование унифицированности параметра противодействия угрозам безопасности определяет ***время*** как наиболее целесообразную форму описания функциональных возможностей СП.

В соответствии с ***требованием иерархии показателей эффективности СП*** предполагается в качестве основы для их систематизации существующая иерархия возможностей СП по решению задач противодействия угрозам безопасности информационной сферы.

Требование оцениваемости показателей предполагает использование единой шкалы для их оценки. В качестве таковой должна быть использована только количественная шкала, позволяющая реализовать оценку с наибольшей точностью.

Требование унификации математического аппарата определяет необходимость формирования математических моделей для анализа всей структуры показателей эффективности СП.

Основными правилами формирования системы показателей эффективности СП являются следующие.

***Правило* 1.** Обобщение показателей эффективности СП должно осуществляться на основе их систематизации. Это правило является следствием необходимости представления показателей эффективности входящих в состав СП средств не простой совокупностью, а в виде системы определенным образом взаимосвязанных элементов оценки их количественных характеристик.

***Правило* 2.** Система показателей эффективности СП при их обобщении должна представляться в виде иерархической структуры. Это правило базируется на предположении, в соответствии с которым обобщение показателей эффективности СП представляет собой поэтапный процесс, начиная с множества частных показателей, отражающих отдельные количественные характеристики конкретных средств СП и заканчивая одним, обобщенным показателем.

***Правило* 3.** Иерархическая структура показателей эффективности СП

представляет собой многоуровневую систему с отношениями "один ко многим".

***Правило* 4.** Многоуровневой структуре системы показателей эффективности СП соответствует унифицированная форма их представления. При этом количественная шкала представления соответствующих показателей может видоизменяться от абсолютной - для оценки показателей нижнего уровня иерархии, до относительной - для оценки показателей верхних уровней иерархии. Следующие два правила конкретизируют данное правило.

***Правило* 5.** Оценка исходного множества частных показателей эффективности СП осуществляется при помощи абсолютной шкалы в форме временных характеристик средств СП.

***Правило* 6.** Оценка промежуточных и результирующего (обобщенного) показателей эффективности СП осуществляется при помощи относительной шкалы. Данное правило определяет круг показателей, оценку которых целесообразно осуществлять в вероятностной форме. К таким показателям следует отнести показатели, которые, в результате обобщения свойств СП, непосредственно определяют цель противодействия угрозам безопасности в критически важных сегментах информационной сферы.

При построении иерархической модели структуры показателей эффективности СП элементы их множества представляются в виде:

$$z_j = \left\langle I_j^{(n)}, v_j, u_j, f_j \right\rangle,$$

где $I_j^{(n)}$ - идентификатор j – го показателя;

v_j - класс возможностей СП, относящийся к данному показателю;

u_j - уровень иерархии в структуре показателей, соответствующий данному классу возможностей СП;

f_j - форма представления показателя, соответствующая данному классу возможностей СП.

***Правило* 7.** Одному уровню структуры соответствует один конкретный класс возможностей СП.

***Правило* 8.** Для произвольных уровней u_k и u_l справедливо условие:

$$u_k > u_l,$$

если свойство k будет более обобщенно, чем свойство l характеризовать степень достижения целей противодействия угрозам безопасности критически важным сегментам информационной сферы. При этом исходное множество S частных показателей эффективности средств СП имеет

уровень, равный единице, а обобщенный показатель *O*, непосредственно характеризующий цель противодействия, самый высокий уровень.

***Правило* 9.** Для произвольных уровней u_k и u_l справедливо условие:

$$\text{если } u_k > u_l, \text{ то } \left|\{y_k(w = u_k)\}\right| \le \left|\{y_l(w = u_l)\}\right|,$$

где $\{y_q(w)\} \in \{z_j\}$ множество показателей w - го уровня.

Свойства СП проявляются при решении соответствующих задач противодействия угрозам безопасности в критически важных сегментах информационной сферы. Сложившаяся к настоящему времени в теории информационной безопасности классификация возможностей по обеспечению защищенности информационной сферы предполагает их деление на четыре класса.

Первый класс задач характеризует возможности элементов информационной сферы, связанные с введением избыточности в средства обработки информации с целью регистрации и регулирования доступа к вычислительным ресурсам компьютерных сетей, криптографического преобразования информации, а также контроля и реагирования на угрозы информационной безопасности. Принимая во внимание требование унификации показателей эффективности противодействия угрозам безопасности, в качестве основы для конструирования частных показателей первого уровня условимся использовать время реализации средствами СП своих функций. При этом под временем $\tau_i^{(1)}$ обеспечения *i*-ой возможности СП по противодействию угрозам безопасности условимся понимать время с момента обращения к средствам СП с целью реализации конкретной функции противодействия до окончания ее реализации.

С точки зрения влияния средств СП на обеспечение защищенности информационной сферы показатели данного уровня отражают самую низкую степень, что позволяет использовать их в качестве исходных при синтезе структуры показателей эффективности СП. В этой связи будет справедливым равенство:

$$\{y_i(w = 1)\} = \{s_i\}.$$

Второй класс задач характеризует возможности, связанные с предупреждением условий появления угроз, поиском, обнаружением и обезвреживанием как самих угроз, так и их источников, а также с восстановлением информации после воздействия угроз. Перечисленные возможности определяются своевременностью реагирования средств СП на угрозы информационной безопасности, что позволяет в качестве основы для конст-

руирования показателей второго уровня использовать своевременность реализации средствами СП собственных функций.

Возможности средств СП по выполнению собственных функций считаются реализованными своевременно, если время $\tau_m^{(2)}$ реализации m-ой возможности по противодействию угрозе информационной безопасности не превышает некоторой максимально допустимой величины $\tau_{(\max)m}^{(2)}$, обусловленной спецификой угрозы, т.е. при выполнении неравенства:

$$\tau_m^{(2)} \le \tau_{(\max)m}^{(2)}. \qquad (1)$$

Следует заметить, что время $\tau_m^{(2)}$ представляет собой функцию от временных характеристик соответствующих возможностей СП применительно к видам обрабатываемой информации, т.е. от показателей первого уровня структуры показателей эффективности СП. То обстоятельство, что времена $\tau_i^{(1)}$ представляют собой случайные величины, приводит к необходимости рассматривать времена $\tau_m^{(2)}$ как их композицию. В этом случае имеет место выражение:

$$\tau_m^{(2)} = \sum_{h=1}^{H} \circ \tau_h^{(1)},$$

в котором $\left\{\tau_h^{(1)}\right\}$, $h = 1, 2, \ldots, H$, $H = \left|\left\{\tau_h^{(1)}\right\}\right|$ - множество временных характеристик (показателей эффективности) СП уровня обеспечения ею возможностей применительно к видам обрабатываемой информации, которые могут быть обобщены показателем $y_m(w=2)$ уровня обеспечения возможностей применительно к отдельным источникам угроз и их действиям (здесь операция $\sum_{h=1}^{H} \circ$ означает композицию H случайных величин).

Максимальное время $\tau_{(\max)m}^{(2)}$ обусловлено активным периодом воздействия угрозы и определяется конкретным вариантом ее реализации.

Входящая в (1) величина $\tau_m^{(2)}$ является случайной. Вероятность события $P_m^{(2)}\left(\tau_m^{(2)} \le \tau_{(\max)m}^{(2)}\right)$ представляет собой среднее количество ситуаций, когда СП своевременно реализуют возможности по противодействию угрозам безопасности информационной сфере в течение интервала ΔT времени ее эксплуатации относительно общего числа таких ситуаций, т.е. имеет место соотношение:

$$P_m^{(2)}(\tau_m^{(2)} \le \tau_{(\max)m}^{(2)}) = \frac{1}{N}\sum_{n=1}^{N}\delta_{m,n},$$

где $\delta_{m,n} = \begin{cases} 1, \ при \ \tau_{m,n}^{(2)} \le \tau_{(\max)m,n}^{(2)} \\ 0, \ при \ \tau_{m,n}^{(2)} > \tau_{(\max)m,n}^{(2)} \end{cases}$;

$\tau_{m,n}^{(2)}$ - время реализации m - ой возможности СП по противодействию n - ой ($n = 1, 2, \ldots, N$) угрозе информационной безопасности информационной сфере;

$\tau_{(\max)m,n}^{(2)}$ - длительность *n*-ой угрозы при использовании m - ой возможности по противодействию;

N - общее число ситуаций возникновения угроз информационной безопасности информационной сфере на временном интервале ΔT.

С учетом изложенного, можно сделать вывод о том, что вероятности $P_m^{(2)}\left(\tau_m^{(2)} \le \tau_{(\max)m}^{(2)}\right),\ m = 1, 2, \ldots, \left|\{y_m(w=2)\}\right|$, достаточно полно характеризуют возможности СП по предупреждению условий появления угроз, поиску, обнаружению и обезвреживанию как самих угроз, так и их источников, а также возможности по восстановлению информации после воздействия угроз. Это позволяет использовать указанные вероятности в качестве обобщенных показателей $y_m(w=2)$ второго уровня, что соответствует выражению:

$$y_m(w=2) = P_m^{(2)}\left(\tau_m^{(2)} \le \tau_{(\max)m}^{(2)}\right).$$

Третий класс характеризует возможности, связанные с предотвращением нарушения конфиденциальности, доступности и целостности информации. Показатели данного уровня обобщают возможности СП, связанные с предупреждением условий появления угроз, поиском, обнаружением и обезвреживанием как самих угроз, так и их источников, а также с восстановлением информации после воздействия угроз. Перечисленные возможности определяются степенью обеспечения СП устойчивости информационной сферы к нарушению состояния информации. Возможности средств СП по обеспечению устойчивости информационной сферы к нарушению конфиденциальности, доступности и целостности информации оцениваются вероятностью $P_n^{(3)}$ противодействия нарушению n-го уровня состояния информации, которая является функцией от вероятностных характеристик соответствующих возможностей СП применительно к отдель-

ным источникам угроз и их действиям, т.е. от показателей второго уровня структуры показателей эффективности СП. В этом случае имеет место выражение:

$$P_n^{(3)} = 1 - \prod_{g=1}^{G} \left(1 - P_g^{(2)} \right),$$

в котором $\left\{P_g^{(2)}\right\}$, $g = 1, 2, \ldots, G$, $G = \left|\left\{P_g^{(2)}\right\}\right|$ - множество вероятностных характеристик (показателей эффективности) СП уровня обеспечения ею возможностей применительно к отдельным источникам угроз и их действиям (этапам проявления), которые могут быть обобщены показателем $y_n(w = 3)$ уровня обеспечения возможностей применительно к нарушениям состояния информации.

Четвертый класс описывает свойство СП, характеризующее степень достижения целей функционирования ее средств – предотвращение ущерба информационной сфере от нарушения безопасности ее критически важных сегментов. Оно выступает в качестве свойства, обобщающего возможности по обеспечению защищенности основных состояний информации.

Соответствующий четвертому уровню структуры показателей эффективности СП показатель является обобщенным и оцениваются вероятностью $P^{(4)}$ обеспечения возможностей противодействия угрозам критически важным сегментам информационной сферы.

Вероятность $P^{(4)}$ является функцией от вероятностных характеристик возможностей СП применительно к нарушениям состояния информации, т.е. от показателей третьего уровня структуры показателей эффективности СП и определяется в соответствии с выражением:

$$P^{(4)} = 1 - \prod_{n=1}^{3} \left(1 - P_n^{(3)}\right),$$

в котором $\left\{P_n^{(3)}\right\}$, $n = 1, 2, 3$ –множество вероятностных характеристик (показателей эффективности) СП уровня обеспечения возможностей применительно к нарушениям состояния информации.

Проведенные исследования дают основания утверждать, что точностные характеристики предложенной иерархической структуры показателей, за счет применения вероятностной шкалы, значительно превосходят точностные характеристики известных интегрированных структур показателей.