А.Ю. Добродеев, А.В. Куликов, Б.П. Пальчун, Е.В. Мишенина
Россия, г. Москва ФГУП «Концерн “Системпром”»,

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Эффект от применения любых систем защиты, и в том числе средств защиты информации (СЗИ), состоит в максимальном предотвращении возможного ущерба от реализации угроз защищаемому объекту. В исследуемом случае таковым объектом являются автоматизированные системы ответственного назначения (АС ОН), предназначенные для управления ответственными, критически важными, иерархически сложными и распределёнными по обширным территориям структурами: транспортными, энергетическими, финансовыми, военными, правоохранительными и т.п. Соответственно ущерб от реализации той или иной угрозы этим объектам определяется (прогнозируется) исходя из конечного негативного результата, т.е., зависит, например, не только от стоимости «испорченного» из-за программного вируса бортового компьютера самолёта и даже не от стоимости потерпевшего по этой причине катастрофу самолёта, а от всех материальных и финансовых потерь, вызванных этой катастрофой. То есть, в основе оценки эффективности СЗИ АС ОН лежит долевой учёт влияния этих СЗИ на результативность действия структуры, управляемых данной АС ОН.

Тогда относительный показатель Э эффективности СЗИ (как и любой системы защиты) в соответствии с положениями теории эффективности определяется следующим выражением [1, 2]:

$$Э = \frac{У - З}{З}, \qquad (1)$$

где У – усреднённая величина предотвращённого ущерба;

З – приведённые затраты на защиту при предотвращении такого ущерба.

Следует отметить, что в современной литературе зачастую под понятием «эффективность СЗИ» понимается та или иная степень защищённости ими объектов информатизации [3, 4], что, по нашему мнению, контрпродуктивно.

Наиболее наглядно выражение (1) «работает» в случае оценки эффективности СЗИ АС ОН финансовыми структурами. Очевидно, что из выражения (1) следует как возможность нулевой эффективности при У = З («СЗИ бесполезно»), так и отрицательной при У < З («СЗИ вредно»).

Для СЗИ АС ОН выражение (1) применимо полностью, но в этом случае весьма сложно установить усреднённую величину предотвращённого ущерба У, причём в тех же единицах измерения и размерности, что и величина З. Кроме того, сложно определить все факторы и количественно оценить соответствующие параметры, влияющие на величины У и З. Но в последнее время появились исследования (например, [5]), посвящённые разработке методологий оценки экономической эффективности АС ОН, которые позволяют производить фактическую финансовую оценку как величины предотвращённого с помощью СЗИ ущерба, так и затрат на мероприятия при предотвращении такого ущерба.

В самом общем виде усреднённая величина предотвращённого ущерба описывается следующей функцией:

$$У = У (\mathbf{Z}, \mathbf{P}_{ру}, \mathbf{P}_{з}, \mathbf{P}_{Т}, \mathbf{P}_{П}), \qquad (2)$$

где $\mathbf{Z}$ – вектор величин возможного (потенциального) ущерба;

$\mathbf{P}_{ру}$ – вектор вероятностей реализации информационных угроз (информационных атак в виде программно - аппаратных воздействий);

$\mathbf{P}_{з}$ – вектор вероятностей защиты информации;

$\mathbf{P}_{Т}$ – вектор показателей технической надёжности СЗИ;

$\mathbf{P_П}$ – вектор показателей надёжности программного обеспечения (компьютерных программ) СЗИ.

Функция У имеет следующие граничные свойства:

при $\mathbf{P_{ру}} = 0$ У = 0;

при $\mathbf{P_з} = 0$ У = 0;

при $\mathbf{P_{ру}} = 1$ и $\mathbf{P_з} = 1$ У равна максимуму;

при $\mathbf{P_Т} = 0$ либо $\mathbf{P_П} = 0$ У = 0.

В свою очередь векторы $\mathbf{Z}$, $\mathbf{P_{ру}}$, $\mathbf{P_з}$, $\mathbf{P_Т}$, $\mathbf{P_П}$ являются сложными функциями, зависящими соответственно от параметров

$$\begin{aligned} &\{\alpha_i\},\ i = 1, \ldots, N_\alpha; \\ &\{\beta_j\},j = 1, \ldots, N_\beta; \\ &\{\gamma_k\},\ k = 1, \ldots, N_\gamma; \\ &\{\eta_m\},\ m = 1, \ldots, N_\eta; \\ &\{\mu_n\},\ n = 1, \ldots, N_\mu. \end{aligned} \qquad (3)$$

Эти параметры характеризуют:

для $\mathbf{Z}$ – структуру и свойства АС ОН, целевое предназначение и свойства управляемого объекта (управляемой структуры), N_α – общее количество объектов (побуждающих факторов) возможного (потенциального);

для $\mathbf{P_{ру}}$ – номенклатуру, иерархически взаимосвязанную структуру и интенсивность угроз информационной безопасности АС ОН, структурную и функциональную уязвимость АС ОН, свойства имеющихся (априорных) СЗИ, N_β – общее количество источников (факторов) угроз информационной безопасности АС ОН;

для $\mathbf{P_з}$ – номенклатуру устанавливаемых СЗИ, вероятностные возможности по противодействию заданным и/или произвольным номенклатурам, структурам и интенсивностям угроз информационной безопасности АС ОН, т.е. $\mathbf{P_з}$ есть некоторая функция и от $\mathbf{P_{ру}}$, N_γ – общее количество СЗИ;

для $\mathbf{P_Т}$ и $\mathbf{P_П}$ – соответственно надёжность каждого отдельного технического устройства и каждой отдельной (самостоятельной) компьютерной программы, входящих в СЗИ, N_η – общее количество технических устройств СЗИ, N_μ – общее количество отдельных компьютерных программ, входящих в состав всех СЗИ.

Кроме того, величина З (приведённые затраты на защиту при предотвращении такого ущерба) есть некоторая функция от вектора параметров

$$\Xi = \{\xi_q\},\ q = 1, \ldots, N_\xi, \qquad (4)$$

где N_ξ – общее количество затратных позиций, описывающих номенклатуру, конструктивные параметры, стоимостные характеристики (закупочные, производственные и эксплутационные) СЗИ, которые зависят в определённой мере от величины $\mathbf{P_з}$ и значит от $\mathbf{P_{ру}}$.

Таким образом, выражение (1) представляет собой сложную многопараметрическую функцию (так называемую функцию эффективности), которая в самой общей форме с учётом (2) – (4)будет иметь следующий вид [6]:

$$Э = \frac{У\left(Z\{\alpha_i\}, P_{ру}\{\beta_j\}, P_з\{\gamma_k\}\right)}{З\left(\{\xi_q\}, P_{ру}\{\beta_j\}, P_з\{\gamma_k\}, P_Т\{\eta_m\}, P_П\{\mu_n\}\right)} - 1. \qquad (5)$$

Естественно, что параметры (3), входящие в состав выражения (5), в сложной взаимосвязи, а все субфункции (2) являются достаточно сложными, поэтому функция эффективности в общем случае имеет полииерархический, симультативный и даже трансцендентный характер. Это, конечно, существенно затрудняет как синтез таких функций в каждом конкретном случае (для сложных АС ОН с современными СЗИ, разумеется), так и их исследование.

Наиболее результативным в этом случае является использование аппарата теории чувствительности, в частности применение следующих коэффициентов

чувствительности: $K_{\alpha i},\ i=1,...,N_\alpha$; $K_{\beta i},\ i=1,...,N_\beta$; $K_{\gamma k},\ k=1,...,N_\gamma$; $K_{\eta m},\ m=1,...,N_\eta$; $K_{\mu n},\ n=1,...,N_\mu$; $K_{\xi q},\ q=1,...,N_\xi$; [7]:

$$
\begin{aligned}
K_{\alpha i} &= \frac{\partial Э}{\partial \alpha_i},\quad i=1,...,N_\alpha;\\
K_{\beta i} &= \frac{\partial Э}{\partial \beta_i},\quad i=1,...,N_\beta;\\
K_{\gamma k} &= \frac{\partial Э}{\partial \gamma_k},\quad k=1,...,N_\gamma;\\
K_{\eta m} &= \frac{\partial Э}{\partial \eta_m},\quad m=1,...,N_\eta;\\
K_{\mu n} &= \frac{\partial Э}{\partial \mu_n},\quad n=1,...,N_\mu;\\
K_{\xi q} &= \frac{\partial Э}{\partial \xi_q},\quad q=1,...,N_\xi.
\end{aligned}
\qquad (6)
$$

где $\frac{\partial Э}{\partial \alpha_i}$, …, $\frac{\partial Э}{\partial \xi_q}$ – частные производные от функции эффективности (5) по параметрам α_i, …, ξ_q для всех определённых значений индексов i, …, q.

Тогда в первом (линейном) приближении приращения функции эффективности из-за вариаций её параметров будут определяться с учётом (6) следующими выражениями:

$$
\begin{aligned}
\Delta Э\alpha_i &= K_{\alpha i}\Delta\alpha_i,\quad i=1,...,N_\alpha;\\
\Delta Э\beta_i &= K_{\beta i}\Delta\beta_i,\quad i=1,...,N_\beta;\\
\Delta Э\gamma_k &= K_{\gamma k}\Delta\gamma_k,\quad k=1,...,N_\gamma;\\
\Delta Э\eta_m &= K_{\eta m}\Delta\eta_m,\quad m=1,...,N_\eta;\\
\Delta Э\mu_n &= K_{\mu n}\Delta\mu_n,\quad n=1,...,N_\mu;\\
\Delta Э\xi_q &= K_{\xi q}\Delta\xi_q,\quad q=1,...,N_\xi,
\end{aligned}
\qquad (7)
$$

где $\Delta Э\alpha_i$, …, $\Delta Э\xi_q$ – приращения функции эффективности при вариациях параметров α_i, …, ξ_q для всех определённых значений индексов i, …, q.

Достоверность построения функции эффективности (5) и вычисления коэффициентов (6) наиболее целесообразно производить с применением имитационной модели, в которой статистическим образом учитываются семантика и структура этой функции, а также значения её параметров [8].

Синтез полномасштабной функции эффективности представляет собой чрезвычайно трудоёмкую задачу (как отмечалось выше, она в общем случае имеет полииерархический, симультативный и даже трансцендентный характер). Эта задача должна решаться в рамках создания общей теории обеспечения информационной

безопасности: без теоретически обоснованного аппарата построения функций эффективности СЗИ любая теория обеспечения информационной безопасности некорректна, а практическая значимость любых методик оценки эффективности СЗИ (в том числе и методики оценки эффективности программно-аппаратных средств маскировки) является интуитивно-эвристической.

В настоящее время нет не только теоретически обоснованной методологии метрологии эффективности СЗИ, но и работоспособной (или хотя бы с внятной метрологией) методологии оценки таких свойств, как «защищённость» или «безопасность» АС (в том числе и АС ОН), т.е. фактически нет легитимного с научной точки зрения аппарата оценки параметров вектора $\mathbf{P}_3$ вероятностей защиты информации. Имеющиеся работы (например, [9–11]) только определяют некоторые подходы к решению этой задачи. Не вдаваясь в подробный анализ этих подходов, следует отметить, что большинство из них даже не принимают в расчёт такое фундаментальное свойство СЗИ, как надёжность их компьютерных программ, не говоря уже об их технологической безопасности в процессе разработки (об учёте возможности внедрения в эти программы закладок самими разработчиками, т.е. об учёте собственной безопасности СЗИ).

Считая необходимым и актуальным незамедлительную интенсификацию работ по созданию теоретических основ построения СЗИ (включая метрологическую теорию эффективности СЗИ), в первую очередь, на базе решения фундаментальных проблем Бородакия [13], в рамках данного исследования функция эффективности СЗИ определяется на основе мультипликативно-аддитивной модели (как модели первичного приближения). Такая модель получается непосредственно из анализа структуры АС ОН и всех её СЗИ с учётом только линейной зависимости от интенсивности информационных атак, стоимостей СЗИ и оценок возможных потерь. Таким образом, полученная функция эффективности (5) будет достаточно наглядной и удобной для исследований с помощью коэффициентов чувствительности (6) и имитационной модели.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кулагин О.А.* Принятие решений в организациях. / Учебное пособие. – СПб.: Сентябрь, 2001. – 139 с.

2. *Петухов Г.Б.,* Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, модели. МО СССР, 1989.

3. *Щеглов А.Ю., Щеглов К.А.* Вопросы оценки эффективности средств защиты компьютерной информации. Комплексный подход к построению средств защиты // Информост. 2006. № 4. июль-август.

4. *Баутов А*. Эффективность защиты информации // Открытые системы. 2003. № 8.

5. *Сухоруков Ю.С., Меркулов С.Н., Фомин В.В.* Методическое обеспечение военно-экономической оценки автоматизированных систем управления тактического звена // Военная мысль. 2007. № 1. – С. 27–38.

6. *Пальчун Б.П., Мишенина Е.В*. Об исследовании функций эффективности систем защиты информации // Труды XI Международной научно-практической конференции «Комплексная защита информации». 20–23 марта 2007. – Новополоцк (Беларусь).

7. Элементы теории испытаний и контроля технических систем / Под ред. Р.М. Юсупова. –Л.: Энергия, 1978. – 192 с.

8. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения: – СПб.: Наука, 1994. – 85 с.

9. Стюгин М. Оценка безопасности системы информационного управления Российской Федерации. – http://www/psyfactor.//org/lib/.

10. *Воробьёв А.А., Куликов Г.В., Непомняших А.В*. Оценивание защищённости автоматизированных систем на основе теории игр // «Информационные технологии».2007. № 1/2.

11. *Буцкий О.Е.* Построение ложных объектов в условиях проведения информационных спецопераций // МИФИ (государственный университет), http://molod.mephi.ru/2002/Data/620htm.

12. *Бородакий Ю.В.* Фундаментальные проблемы теории информационной безопасности автоматизированных систем // Труды VIII Международной конференции «Комплексная защита информации». 23–26 марта 2004. – Валдай.

А.В. Благодаренко
Россия, г. Таганрог, Технологический институт ЮФУ

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ДЛЯ ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БЕЗ ИСХОДНЫХ КОДОВ

В настоящее время стремительного развития информационных технологий и глобальной компьютеризации человеческой жизни на передний план выходит зависимость человека от компьютерных программ. Их корректная работа и неподверженность удаленным атакам все больше и больше волнует пользователей, так как множество личной и ценной информации хранится на электронных носителях. Лабораторные сертификационные испытания призваны определить степень доверия пользователя к программному обеспечению. При проведении испытаний сертификационные лаборатории опираются на Руководящий документ (РД) Гостехкомиссии России по контролю над недекларированными возможностями [1]. Данный документ предписывает проводить анализ исследуемого ПО по исходным текстам. Однако существуют ситуации, когда исходные тексты для ПО недоступны. Например, если ПО распространяется свободно и автор находится за границей[2]. В такой ситуации сертификация может быть проведена и по исполняемому коду. В настоящее время, однако, для подобных испытаний нет соответствующей нормативной базы. Инструментальные средства для анализа ПО без исходных кодов есть, но они не удовлетворяют всем требованиям к проведению сертификационных испытаниях (если ввести в РД допущение на сертификацию ПО без исходных кодов). В табл. 1 рассматривается пригодность использования различных программных средств для проведения анализа ПО без исходных кодов.

Таблица 1

Пригодность существующих инструментальных средств для проведения сертификационных испытаний ПО без исходных кодов

Инструментальное средство	Недостатки
Аист - С	Ограниченность языком С/С++ Только статический анализ
EMU	Виртуальная среда Отсутствие статического и динамического анализа
SoftIce	Минимальный статистический анализ Отсутствие динамического анализа
IDA	Только статический анализ

Первые два средства из представленных в таблице («Аист-С» и «EMU») являются рекомендованными для проведения сертификационных испытаний ПО[2]. «Аист-С» представляет собой довольно мощный инструмент для анализа исходных кодов С/С++ с возможностью построения трасс, графов взаимодействия функциональных единиц и оценки избыточности. Выполнение тех же действий над ПО без исходных кодов требует сочетания разных инструментальных средств.