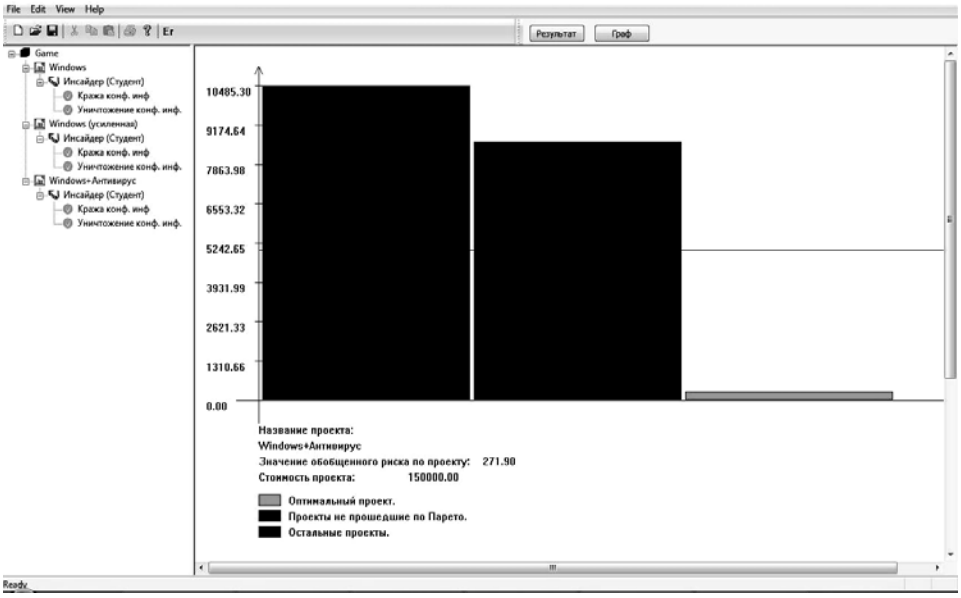

Рис. 2. Результаты моделирования (экранная копия)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Петренко С.А. Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс. 2004.

2. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания – М.: КомКнига, 2005.

3. *Кельтон В., Лоу А*. Имитационное моделирование. Классика CS. 3-е издание. – СПб.: Питер; Киев: Издательская группа BHV, 2004.

4. *Протасов И.Д.* Теория игр и исследование операций: Учебное пособие. – М.: Гелиос АРВ, 2003.

УДК 681.3.034

С.Г. Данилюк, В.Г. Маслов

ОБОСНОВАНИЕ НЕЧЕТКОГО СИТУАЦИОННОГО ПОДХОДА К СОЗДАНИЮ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЛОЖНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

Бурное развитие информационных технологий и внедрение последних в процессы управления критически важными системами привело к острой необходимости защиты информационных ресурсов от злонамеренного вторжения с целью вывода их из строя или получения доступа к информации ограниченного пользования. Указанная проблема привела к необходимости поиска путей и решений защиты информационных систем от деструктивного, как внешнего так и внутреннего воздействия. Защита информационных систем – сложная комплексная задача, призванная решать вопросы обеспечения конфиденциальности, целостности и доступности информации. Решение вопроса обеспечения защиты информации может достигаться как программными (межсетевые экраны, анализаторы уязвимостей

программных продуктов и сетей, встроенные средства защиты операционных систем), так и программно-аппаратными средствами (отчуждаемые носители, криптографические ключи и замки и др.).

Современные информационные системы характеризуются, в большей степени, распределенным характером, вследствие этого основным потенциальным источником угроз является угрозы перехвата транслируемого трафика, его анализа и принятия вредоносного решения по результатам перехвата.

Основными видами вредоносного воздействия по результатам перехвата могут быть:

- простое прослушивание сети (возможно по причине отсутствия физической защиты линий передачи информации, отсутствие криптозащиты). Данный вид вредоносного воздействия носит пассивный характер;

- внедрение в распределенную сеть ложного информационного объекта со стороны злоумышленника, передача вредоносного трафика в информационную систему от имени реального (легального) объекта (субъекта), перенаправление легального трафика по ложному маршруту, модификации транслируемой в сети информации. Данный вид вредоносного воздействия носит активный характер;

- атакующее воздействие на информационную систему со стороны злоумышленника с целью передачи в систему паразитного трафика – провоцирования отказа в обслуживании легальных пользователей. Данный вид вредоносного воздействия носит активный характер;

- модификация (изменение) критически важных легальных ресурсов, составляющих информационные системы, в том числе модификация от лица легальных пользователей. Данный вид вредоносного воздействия носит активный характер и др.

При рассмотрении модели потенциального нарушителя информационных систем следует иметь ввиду субъективный характер вредоносного воздействия. Нарушитель (хакер), как правило, имеет средний уровень квалификации в области информационных технологий, а также имеет определенные навыки использования средств автоматизации поиска уязвимостей информационных систем и средств взлома программного обеспечения. Нарушитель принимает решение об использование путей проникновения в систему на основании сведений, полученных в процессе анализа степени защищенности системы. Кроме того, при рассмотрении модели нарушителя следует принимать во внимание уровень его адекватности, насколько глубоко последний осознает степень своей ответственности за последствия взлома систем, включая и уголовную ответственность, а также соответствие результатов, полученных от взлома поставленным злоумышленником целям.

Уровень защиты информационной системы определяется видом воздействия злоумышленника, его глубиной и интенсивностью. В задачу систем защиты информационных ресурсов входит анализ уровня вредоносного воздействия со стороны злоумышленника и принятия адекватного решения – противодействия вторжению по результатам анализа. В любом случае, чем больше степеней (эшелонов) защиты имеет система, тем сложнее злоумышленнику нанести реальный вред ее информационным ресурсам.

Основываясь на субъективном характере вредоносного воздействия на защищаемые информационные ресурсы вполне допустимо вести речь о его нечетком характере, и, как следствие, модель противодействия вторжению в информационную систему также может носить нечеткий характер.

Одним из подходов защиты информационных объектов является ввод в заблуждение (дезинформирование) потенциальных нарушителей границ информа-

ционных систем относительно истинных характеристик, целей, задач, решаемых информационным объектом. Указанный подход может достигаться различными путями, в том числе и путем создания ложных информационных объектов.

Ложный информационный объект распределенной информационной системы представляет собой аналог реального информационного объекта, которому свойственны основные функциональные характеристики реального. При рассмотрении информационной системы в целом следует вести речь о совокупности определенного количества ложных информационных объектов, как одной из составляющих элементов системы защиты информационных ресурсов. Количество ложных информационных объектов, их структурный состав, а также уровень противодействия вторжению в свою очередь должен соответствовать глубине и интенсивности вредоносных атак. С учетом нечеткого характера модели злонамеренного воздействия на информационную систему вполне допустимо говорить и о нечеткой модели системы противодействия злонамеренному воздействию на основе ложных информационных объектов. В свою очередь нечеткий характер поведения объектов (субъектов) в достаточной степени хорошо может быть описан на базе элементов теории нечетких множеств.

Исходными данными для формирования системы защиты информации на базе совокупности ложных информационных объектов, как отмечалось ранее, является глубина и интенсивность вредоносного воздействия злоумышленников. Глубина и интенсивность атакующего воздействия может характеризоваться рядом параметров, набор которых может отличаться от атаки к атаке. Для того чтобы оценить степень (значение) возможного ущерба, наносимого информационной системе, необходимо выработать общий принцип оценки важности (весомости) того или иного параметра, которую можно провести на основании совокупности критериев.

Среди параметров, имеющих нечисловую структуру, характеризующих вредоносное атакующее воздействие, целесообразно выделить параметры двух различных типов, а именно параметры качественной оценки и параметры, характеризующие степень влияния оценок по соответствующим показателям на общую оценку возможного ущерба информационной системе.

Для обозначения указанного типа параметров введем лингвистические переменные y_i = «ПАРАМЕТР $_i$» и z_k = «ЗНАЧИМОСТЬ $_k$». Лингвистическую переменную y_i = «ПАРАМЕТР $_i$» будем использовать для обеспечения возможности формализации качественной информации детерминированного характера. При этом в соответствии с принятыми соглашениями [3] будем рассматривать каждый параметр $y_i \in Y$ как лингвистическую переменную $\langle y_i, T_i, D_i \rangle$ с названием «ПАРАМЕТР $_i$». Для формализации информации о значимости (вкладе) каждого параметра в общую оценку будем использовать лингвистическую переменную $\langle z_k, S_k, H_k \rangle$ с названием «ЗНАЧИМОСТЬ $_k$».

Ключевым моментом в разработке лингвистических переменных «ОЦЕНКА» и «ЗНАЧИМОСТЬ» является построение их терм-множеств. Необходимость создания условий для обеспечения требуемой глубины, полноты и интенсивности оценки вредоносного воздействия со стороны нарушителя границ информационной системы является исходным пунктом для решения задачи по разработке лингвистических переменных «ОЦЕНКА» и «ЗНАЧИМОСТЬ», является задача формирования их терм-множеств и определение смысла вошедших в них термов.

Терм-множество лингвистических переменных «ОЦЕНКА» и «ЗНАЧИМОСТЬ» должно представлять собой совокупность термов, удовлетворяющих следующим условиям [2]:

$$\begin{cases} \mu_{C_1}(\inf D)=1, \\ \mu_{C_J}(\sup D)=1, \\ \forall T_j \in T \setminus \{T_J\} \quad 0<\sup \mu_{C_j \cap C_{j+1}}(d)<1, \\ \forall T_j \in T \quad \exists d \in D \left| \mu_{C_j}(d)=1, \right. \\ \exists d_1, d_2 \in D \left| \forall d \in D \left(d_1 < d < d_2\right). \right. \end{cases}$$

где $T=\left\{T_j \left| j=\overline{1,J} \right.\right\}$ – упорядоченное терм-множество в соответствии с правилом:

$$\forall T_j, T_k \in T(j>k) \Leftrightarrow \exists d_j, d_k \in D\left(d_j > d_k\right) ,$$

означающим, что терм, который имеет левее расположенный носитель, получает меньший номер. Это условие означает, что понятия, используемые в качестве значений лингвистических переменных «ОЦЕНКА» и «ЗНАЧИМОСТЬ», должны составлять множество, упорядоченное по возрастанию качественных значений признака.

Для определения семантики значений лингвистических переменных, каждая из которых в свою очередь является нечеткой переменной, необходимо выбрать способ, с помощью которого будет формализована информация о глубине и интенсивности вторжения в систему. При этом за основу возьмем способ, основанный на использовании функции принадлежности, как некоторой функции, которая отображает элементы базового множества $d_i \in D$ в интервал [0, 1], характеризуя субъективную степень их соответствия формализуемому понятию.

В качестве способа построения функций принадлежности нечетких множеств будем использовать π-функцию, определяемую следующей системой выражений [1]:

$$\mu_{C_j}(d)=\pi\left(d, \eta_j, d_j^{\text{л}}, d_j^{\text{п}}\right)^{2^{\varphi}},$$

$$\pi\left(d, \eta_j, d_j^{\text{л}}, d_j^{\text{п}}\right)=\begin{cases} s\left(d, d_j^{\text{л}}-2\eta_j, d_j^{\text{л}}-\eta_j, d_j^{\text{л}}\right), \text{ при } d \le d_j^{\text{л}}, \\ 1, \text{ при } d_j^{\text{л}} \le d \le d_j^{\text{п}}, \\ 1-s\left(d, d_j^{\text{п}}, d_j^{\text{п}}+\eta_j, d_j^{\text{п}}+2\eta_j\right), \text{ при } d \ge d_j^{\text{п}}, \end{cases}$$

$$s\left(d, \xi, \tau, \delta\right)=\begin{cases} 0, \text{ при } d \le \xi, \\ \dfrac{2(d-\xi)^2}{(\delta-\xi)^2}, \text{ при } \xi \le d \le \tau, \\ 1-\dfrac{2(\delta-d)^2}{(\delta-\xi)^2}, \text{ при } \tau \le d \le \delta, \\ 1, \text{ при } d \ge \delta. \end{cases}$$

При таком задании функция принадлежности $\mu_{C_j}(d)$ может быть представлена в памяти ЭВМ четырьмя параметрами: $d_j^{л}$ и $d_j^{п}$, задающими интервал номинальных значений базовой переменной *d*, степень принадлежности которых терму $T_j \in T \setminus \{T_1, T_J\}$ равна 1; η_j определяющим относительно значений $d_j^{л}$ и $d_j^{п}$ базовые значения *d*, степень принадлежности которых терму $T_j \in T \setminus \{T_1, T_J\}$ равна 0,5; параметром φ, характеризующим функцию принадлежности в промежутках:

$$\left[d_j^{л} - 2\eta_j; d_j^{л}\right], \ \left[d_j^{п}; d_j^{п} + 2\eta_j\right].$$

При необходимости получения числовых оценок для значений лингвистических переменных целесообразно воспользоваться методом полной интерпретации [3]. В основе метода полной интерпретации лежит определение «центра тяжести» нечеткого множества в соответствии с приведенными ниже выражениями:

$$\hat{T} = \frac{\int\limits_{d=d^{л}-2\eta^{л}}^{d^{п}+2\eta^{п}} d\,\mu_T(d)\ \mathrm{d}d}{\int\limits_{d=d^{л}-2\eta^{л}}^{d^{п}+2\eta^{п}} \mu_T(d)\ \mathrm{d}d}.$$

Процедура полной интерпретации позволяет переходить от функций принадлежности, формализующих значения лингвистических переменных (нечеткие переменные), к точным числовым оценкам, компактно характеризующим суть используемых в процессе оценивания возможного ущерба понятий, т.е. к конкретным значениям оценок параметров и их влияние на совокупное значение возможного ущерба.

На основании указанного подхода, информационная система, обладающая определенной степенью самостоятельности принятия решения (обладая элементами искусственного интеллекта), в состоянии определить степень, глубину и интенсивность атакующего вредоносного воздействия, и по результатам анализа принять решение о генерировании определенного числа ложных сетевых информационных объектов, а также определить сложность их структуры.

Структура типового ложного информационного объекта формируется на основании модели поведения нарушителя системы и предусматривает возможность компоновки ложного объекта из типового набора сервисов и служб в зависимости от оценки информационной системой уровня атакующего воздействия. Очевидно, что чем выше степень опасности вредоносного воздействия, тем сложнее должна быть структура ложного сетевого объекта и больше их количество генерироваться в системе.

Указанный подход оценивания уровня потенциальной угрозы информационным системам может быть использован и в других сферах обеспечения политики информационной безопасности, где поведение объектов (субъектов) может быть смоделировано на основании нечеткого ситуационного подхода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Данилюк С.Г.* Вероятностно-лингвистический метод диагностирования: Учебное пособие. – Серпухов: МО РФ, 1998. – 96 с.
2. Классификация и кластер / Под ред. Дж.Райзина. – М.: Мир, 1980.
3. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д.А. Поспелова. – М.: Наука, 1986. – 312 с.

УДК 681.354

М.Е. Путивцев

АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕССНОГО ПОДХОДА*

Обеспечение информационной безопасности (ИБ) компьютерных систем различного назначения продолжает оставаться чрезвычайно острой проблемой. Можно констатировать тот факт, несмотря на усилия многочисленных организаций, занимающихся решением этой проблемы, общая тенденция остается негативной. Основных причин этому две:

– возрастающая роль информационных технологий в поддержке бизнес-процессов, как следствие возрастающие требования к ИБ автоматизированных систем. Цена ошибок и сбоев информационных систем возрастает;

– возрастающая сложность информационных процессов. Это предъявляет повышенные требования к квалификации персонала, ответственного за обеспечение ИБ. Выбор адекватных решений, обеспечивающих приемлемый уровень ИБ при допустимом уровне затрат, становится все более сложной задачей.

Аудит информационной безопасности является одним из наиболее актуальных и динамично развивающихся направлений менеджмента в области информационной безопасности (ИБ). Его основной задачей является объективная оценка текущего состояния информационной безопасности организации, а также ее адекватность поставленным целям и задачам бизнеса с целью увеличения эффективности и рентабельности экономической деятельности предприятия [1]. Результаты качественно выполненного аудита позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Основные задачи проведения аудита безопасности включают в себя:

- контроль эффективности затрат на системы информационной безопасности;
- проверка плановых этапов развития СУИБ;
- контроль соблюдения интеллектуальной собственности;
- инвентаризация и детализация информационных ресурсов (финансовые отчеты, планы);
- определения законности и эффективности использования информационных ресурсов;
- выявление недостатков с точки зрения информационной безопасности;
- устранение недостатков и внесение необходимых рекомендация;
- выявление нарушений в АСУ.

В настоящее время существует довольно большое количество как отечественных, так и зарубежных методик и подходов по проведению аудита информаци-

* Работа выполнена при поддержке гранта РФФИ №07-07-00138а.