УДК 681.14

# АЛГОРИТМ ОЦЕНКИ ВЕРОЯТНОСТИ ВТОРЖЕНИЙ ДЛЯ СРЕДСТВ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

**В.Е. МУХИН, А.Н. ВОЛОКИТА**

Предложен новый алгоритм оценки вероятности вторжений для средств мониторинга безопасности в компьютерных системах, который предусматривает проведение анализа целей вторжений, ранжируемых по степени угроз безопасности компьютерным системам, что позволяет сформировать дифференциальную оценку вероятности этих вторжений. Разработанный алгоритм обеспечивает повышение эффективности функционирования систем мониторинга безопасности, построенных на его основе.

## ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ МОНИТОРИНГА БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Высокая степень информатизации, которая характеризует современное общество, обусловливает зависимость его безопасности от защищенности используемых информационных технологий. Широкое применение компьютерных систем (КС), позволившее решить задачу автоматизации процессов обработки постоянно возрастающих объемов информации, сделало эти процессы особенно уязвимыми по отношению к агрессивным воздействиям и атакам, что породило новую проблему — информационную безопасность.

Опыт эксплуатации современных КС показывает, что проблема информационной безопасности еще не решена, ввиду того, что средства защиты не в состоянии предотвратить нарушения, число которых растет год от года. Необходима разработка новых подходов к созданию средств защиты информации, способных обеспечить адекватное противодействие современным угрозам и удовлетворить постоянно возрастающим требованиям к безопасности КС и сетей.

Одним из ключевых механизмов защиты информации в современных КС и сетях являются средства мониторинга безопасности, которые реализуют наблюдение, анализ и прогнозирование состояний безопасности КС. Они выполняют предварительный анализ, оперативный контроль и реализацию механизмов реакции на вторжения в КС, что обеспечивает выявление атак злоумышленников и упреждающее формирование комплекса мер по локализации возможных несанкционированных действий в системе.

Эффективность системы мониторинга безопасности КС (СМБ КС) во многом определяется корректностью реализации. Одним из важнейших ее элементов является алгоритм оценки состояния контролируемого объекта для формирования реакции средств мониторинга безопасности на потенциально опасные действия в системе [1, 2].

Таким образом, всесторонний анализ современных СМБ требует оценки свойств алгоритмов формирования вероятности вторжений в КС, используемых при реализации средств мониторинга безопасности [3].

В настоящее время существует несколько основных подходов к реализации средств мониторинга безопасности [4], которые используют:

1. **Статистический анализ.** Накапливается статистическая информация о действиях субъектов. В дальнейшем она сравнивается с показателями нормального поведения легальных субъектов или, наоборот, действий, характерных для вторжения. Недостатки данного подхода — субъективный фактор (эксперты), неоднозначная трактовка получаемых результатов и отсутствие возможности адаптивной настройки системы.

2. **Экспертная система.** Принимает решения о принадлежности того или иного события к классу атак на основании сформированных правил. Недостатки этого подхода — высокая сложность практической реализации системы и субъективные экспертные оценки.

3. **Искусственные нейронные сети.** Обучаются специальным образом, чтобы идентифицировать типичные характеристики вторжений или статистически значимые отклонения от нормального режима работы субъектов. Свойства СМБ на основе данного подхода определяются характеристиками аппарата нейронных сетей, которые представляют собой так называемый «черный ящик», что обусловливает вероятность получения необъяснимых или некорректных результатов.

В целом, для всех известных подходов к построению СМБ КС характерны следующие недостатки:

- Существующие СМБ не способны точно идентифицировать злоумышленника, определить его конечную цель и мотив поступков. В общем случае они лишь блокируют действия злоумышленника, что в будущем может привести к повторным атакам [5].
- Алгоритмы формирования вероятности вторжений в СМБ КС оперируют сокращенным вектором опасных действий, сформированным лишь на основании данных самой системы.
- При определении вероятности вторжения злоумышленников в КС или сеть не выполняется автоматическое ранжирование угроз их действий путем анализа потенциального ущерба системе.
- События, связанные с безопасностью КС, инициаторы которых не выявлены, в дальнейшем игнорируются [6,7].
- Алгоритмы формирования вероятностей вторжений не предусматривают прогнозирования действий нарушителя, которое позволяет сформировать «ложные уязвимости» для злоумышленника.

Таким образом, разработка новых алгоритмов анализа вероятности вторжений в СМБ, позволяющих устранить или существенно снизить представленные выше характерные недостатки, является актуальной.

## УЛУЧШЕННЫЙ АЛГОРИТМ ОЦЕНКИ ВЕРОЯТНОСТИ ВТОРЖЕНИЙ НА ОСНОВЕ АНАЛИЗА ЦЕЛЕЙ ЗЛОУМЫШЛЕННИКОВ ДЛЯ СИСТЕМ МОНИТОРИНГА БЕЗОПАСНОСТИ

На основании анализа существующих подходов и алгоритмов мониторинга безопасности предлагается новый алгоритм оценки вероятности вторжений в КС, в котором учитываются цели злоумышленников и выполняется группировка их действий по определенным признакам.

В данном алгоритме для формирования вероятности вторжений в КС используется расширенный сеансовый вектор $\mathbf{X} = \{x_1, x_2, ..., x_n\}$, представляющий собой счетчики факторов различных угроз безопасности $x_i$, зафиксированные средствами сбора информации и проверки состояния КС.

В существующих подходах вектор $\mathbf{X}$ характеризуется дублированием факторов и, как следствие, их избыточностью, а также высокой детализацией учитываемых параметров угроз, что усложняет дальнейшую его обработку. В предложенном алгоритме выполняется группирование факторов $x_i$ отдельных, в том числе низкоуровневых, действий нарушителя в более высокоуровневые события нарушения безопасности, и формируется вектор действий $\mathbf{A}$ (рис. 1).

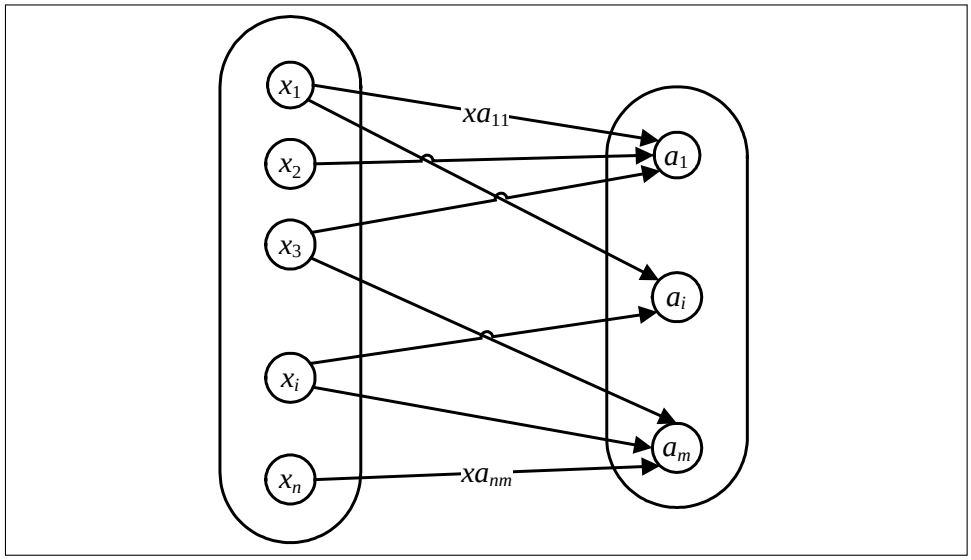


*Рис. 1.* Группирование элементов вектора $\mathbf{X}$ в вектор действий $\mathbf{A}$

Элементы вектора $\mathbf{A}$ рассчитываются как

$$a_j = \sum_{i=1}^{n} x_i \, xa_{ij}, \qquad (1)$$

где $xa_{ij}$ — элемент матрицы преобразования

$$\mathbf{XA} = \begin{bmatrix} xa_{11} & \dots & xa_{1m} \\ \dots & & \dots \\ xa_{n1} & \dots & xa_{nm} \end{bmatrix},$$

причем $xa_{ij}$ — коэффициент, соответствующий весу фактора $x_i$ в конечном действии $a_j$ субъекта.

В общем виде выражение (1) можно записать так:

$$\mathbf{A} = F_{xa}(X), \tag{2}$$

где $F_{xa}$ — функция преобразования вектора $\mathbf{X}$ в вектор $\boldsymbol{A}$.

Формирование вектора $\mathbf{A} = \{a_1, a_2, \ldots, a_m\}$ в соответствии с (1) позволяет минимизировать объем обрабатываемой информации за счет группирования факторов действий субъектов и при этом, как будет показано далее, более корректно анализировать ее по сравнению с использованием обычного порогового вектора $\mathbf{X}$.

Вначале коэффициент $xa_{ij}$ определяется на основе статистических данных о действиях субъектов в КС и экспертных оценок, затем он автоматически обновляется по следующему принципу: коэффициент $xa_{ij}$ того фактора $x_i$, который оказывает большее/меньшее влияние при осуществлении соответствующего действия $a_j$, увеличивается/уменьшается на величину $\Delta_{ij}$ по формулам

$$xa_{ij\,\text{нов}} = xa_{ij} + \Delta_{ij}, \tag{3}$$

$$\Delta_{ij} = \frac{x_{i\,\text{нов}} - x_i}{a_j}\delta, \tag{4}$$

где $\Delta_{ij}$ — коррекция веса фактора $x_i$ в действии $a_j$; $xa_{i\,\text{нов}}$ — значение веса фактора $x_i$ в действии $a_j$ после коррекции; $x_{i\,\text{нов}}$ — новое значение фактора $x_i$; $\delta$ — коэффициент настройки факторов.

Кроме того, предложенный алгоритм позволяет модифицировать состав групп факторов $\{x\}$ для вектора $\mathbf{A}$, но решение об включении/исключении факторов принимает администратор.

Таким образом, параметры вторжения представляются в виде кортежа данных

$$\{s_1,..,s_n\},\ \{t_1,...,t_c\},\ \{l_1,...,l_d\},\ \{m_1,...,m_e\},\ \{\gamma_1,...,\gamma_f\},$$

где $s_i$ — субъект инициатор события; $t_i$ — время события; $l_i$ — место события; $m_i$ — задействованные средства; $\gamma_i$ — степень успешности вторжения.

Далее производится импликация действий субъектов в их цели (рис. 2).

Данное преобразование позволяет прогнозировать возможный следующий шаг субъекта за счет установления корреляционной зависимости между целью $g_j$ и набором действий $\{a\}$, необходимых для ее достижения. Важность выполнения этого преобразования обусловлена тем, что набор формально несвязанных действий может преследовать общую цель.

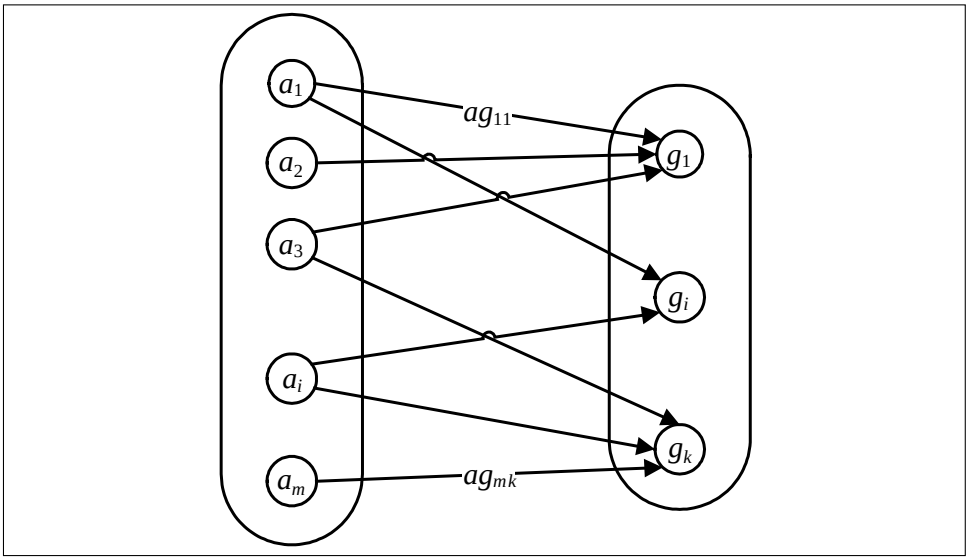


*Рис. 2.* Импликация вектора **A** в вектор целей **G**

Элемент $g_j$ вектора целей **G** рассчитывается как

$$g_j = \sum_{i=1}^{m} a_i \, a g_{ij} \,, \tag{5}$$

где $ag_{ij}$ — коэффициент, показывающий вес действия $a_i$ субъекта в достижении цели $g_j$. Данный коэффициент — это элемент весовой матрицы **AG**, которая формируется на основании экспертных оценок и статистических данных о действиях субъектов.

$$\mathbf{AG} = \begin{bmatrix} ag_{11} & \dots & ag_{1k} \\ \dots & & \dots \\ ag_{m1} & \dots & ag_{mk} \end{bmatrix}.$$

Аналогично обновлению коэффициентов $xa_{ij}$ выполняется автоматическое обновление коэффициентов $ag_{ij}$ на основании статистики о действиях субъектов в КС.

В общем виде выражение (5) можно представить как

$$\mathbf{G} = F_{ag}(A) \,, \tag{6}$$

где $F_{ag}$ — функция преобразования вектора **A** в вектор **G**.

На следующем этапе на основе информации о существующих причинно-следственных связях, указывающих на взаимосвязь между вторжениями, дифференцированными по времени, месту, способу атаки и задействованным средствам, строится вероятностный граф потенциальных целей нарушителей (рис. 3).

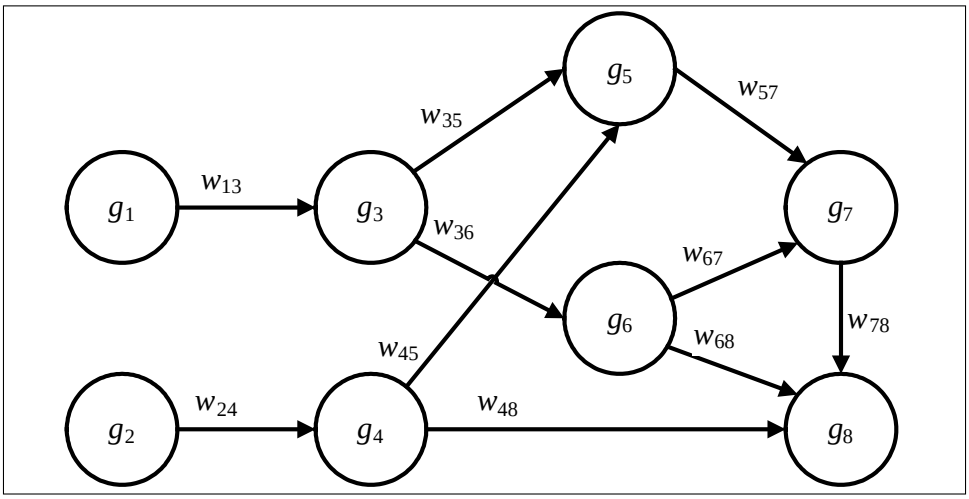


*Рис. 3.* Вероятностный граф потенциальных целей субъектов

Данный граф описывает последовательность потенциальных целей нарушителей для реализации вторжений. Вершины графа $g_i$ представляют собой цели, достижение которых позволяет оказывать определенное воздействие на КС, а дуги $w_{ij}$ — вероятности, показывающие степень возможности перехода от одной цели к другой. Граф целей позволяет выстроить цепочку возможных действий злоумышленника, исходя из его текущего положения в пространстве целей и текущей активности, а также спрогнозировать его следующие шаги и определить потенциальные и возможные конечные цели и, соответственно, возможные действия.

Так, если известны потенциальные цели злоумышленника, то соответствующие им действия $a_i$ могут быть получены из

$$\mathbf{A} = F_{ag}^{-1}(G), \tag{7}$$

а факторы $x_i$ различных угроз безопасности, которые при этом необходимо контролировать, из

$$\mathbf{X} = F_{xa}^{-1}(A), \tag{8}$$

где $F_{ag}^{-1}$ и $F_{xa}^{-1}$ — функции обратного преобразования относительно функций $F_{ag}$ и $F_{xa}$, соответственно.

Полученный прогноз поведения нарушителя может быть использован для эмуляции уязвимостей и системных сведений (маскарад). Причем в зависимости от характера действий и целей злоумышленника могут применяться как сокрытие и дезинформация, так и полная подмена критичных данных.

Задача средств защиты информации состоит в обеспечении безопасности информационных ресурсов КС. Таким образом, необходимо установить соответствие между целями злоумышленника и ресурсами, которые будут подвержены атакам при реализации этих целей.

На рис. 4 показано отражение набора целей $\{g\}$ злоумышленников на те информационные ресурсы $\{r\}$ КС, которые будут подвержены воздействию.

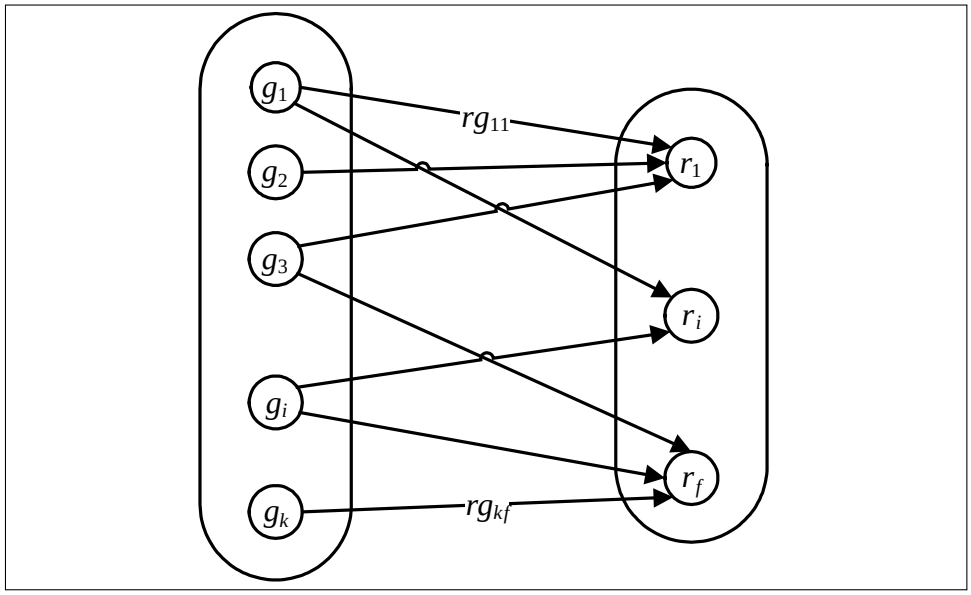


*Рис. 4.* Отражение набора целей $\{g\}$ субъектов на ресурсы $\{r\}$ КС

Значение вектора конкретных информационных ресурсов

$$R_{1\times f} = G_{1\times k} \times \left\| GR_{k\times f} \right\|, \tag{9}$$

где $G_{1\times k}$ — вектор целей; $GR_{k\times f}$ — матрица преобразования, коэффициенты $gr_{ij}$ которой отражают влияние достигнутых злоумышленником целей $g_i$ в воздействии на информационный ресурс $r_j$ КС.

На рис. 5 показан полный цикл преобразования действий нарушителя $a_i$ с помощью формирования соответствующих им наборов целей $\{g\}$ в элементы вектора $\{r\}$, отражающие степень угрозы действий $\{a\}$ субъектов для конкретных информационных ресурсов $\{r\}$ КС.

Информационная ценность ресурса $r_1$ определяется выражением

$$r_1 = g_1 gr_{11} + g_4 gr_{41}, \tag{10}$$

что эквивалентно

$$r_1 = (a_1 ag_{11} + a_2 ag_{21} + a_3 ag_{31}) gr_{11} + \\ + (a_3 ag_{34} + a_6 ag_{64}) gr_{41}. \tag{11}$$

Информационная ценность $r_i$ ресурса прямо пропорциональна вероятности вторжения $p_i$ злоумышленника в КС.

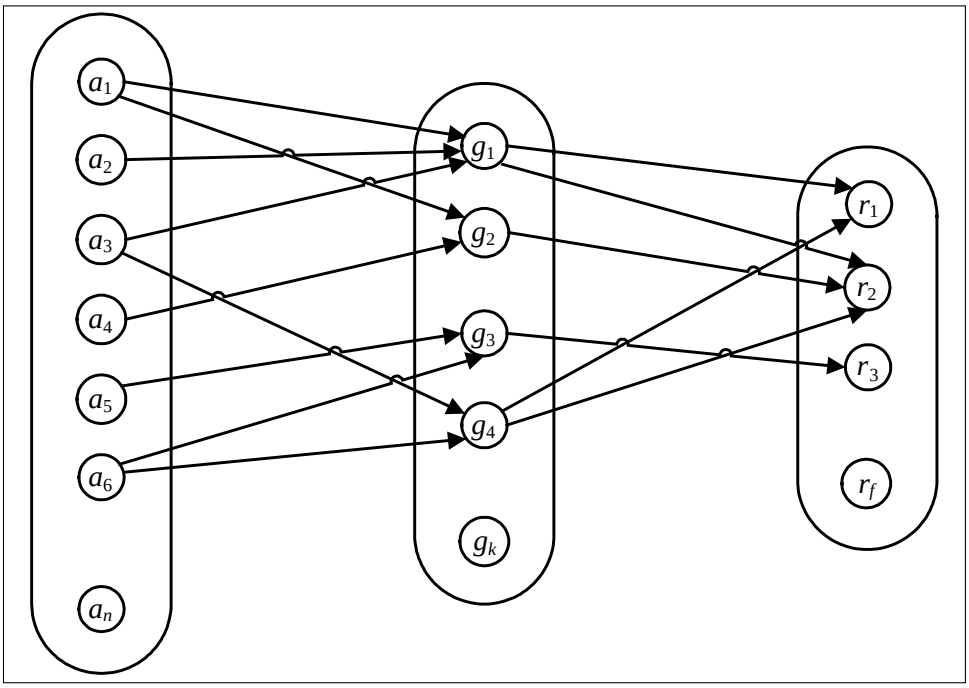


*Рис. 5.* Зависимость между действиями нарушителя $\{a\}$ и ресурсами $\{r\}$ КС, подвергающимися атакам

Предложенный подход позволяет определить потенциальную ценность $r_{1\text{нов}}$ ресурса $r_i$ с помощью вероятностного графа целей (см. рис. 3). Так, например, если цель $g_4$ еще не достигнута, то

$$r_{1\text{нов}} = r_1 + (g_2 w_{24})\, g r_{41}. \qquad (12)$$

Как видно из соотношения (12), потенциальная ценность данного ресурса КС больше или равна его текущей ценности.

Текущая информационная ценность ресурса уменьшается в том случае, если цели злоумышленников (соответственно и их действия) не направлены на данный информационный ресурс. Далее в предложенном алгоритме формируется дифференциальная оценка вероятности вторжений $p_i$ в КС, учитывающая ранжирование состояний КС, которая определяется как вероятность воздействия на ресурс $r_i$, с учетом коэффициента нормирования $k_i$.

$$p_i = k_i\, r_i. \qquad (13)$$

Коэффициент нормирования $k_i$ — параметр для приведения диапазона значений, полученных при анализе возможных воздействий на информационный ресурс, к интервалу [0…1]. Для различных ресурсов значения коэффициента $k_i$ отличаются и зависят от их ценности, критичности и важности для работы всей системы в целом.

На конечном этапе алгоритма собираются полученные данные по ряду сеансов работы субъектов и определяется квота подозрительности действий

нарушителей, а также формируется степень угрозы информационным ресурсам.

Предложенный алгоритм позволяет ранжировать действия и цели субъектов по степеням их угроз безопасности КС, что, в свою очередь, обеспечивает дифференциальную оценку вероятности вторжения в зависимости от ценности информационного ресурса.

## ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ СРЕДСТВ МОНИТОРИНГА БЕЗОПАСНОСТИ, ПОСТРОЕННЫХ НА ОСНОВЕ РАЗЛИЧНЫХ АЛГОРИТМОВ ОЦЕНКИ ВЕРОЯТНОСТИ ВТОРЖЕНИЙ В КС

Для оценки эффективности функционирования предложенного алгоритма оценки вероятности вторжений для СМБ КС проведены экспериментальные исследования его характеристик.

Выполнено моделирование функционирования четырех различных алгоритмов анализа вероятности вторжений в КС, входящих в состав четырех различных СМБ:

1) использующей статистический алгоритм обнаружения аномального поведения (система типа I);

2) имеющей встроенную экспертную систему (типа II);

3) построенной с использованием нейросетевых технологий (типа III);

4) созданной на основе предложенного алгоритма оценки вероятности вторжений в КС (типа IV).

Вероятность корректной работы СМБ

$$P = 1 - \max\{P_{\mathrm{I}}, P_{\mathrm{II}}\}, \qquad (14)$$

где $P_{\mathrm{I}}$ — вероятность ошибки I рода (отсутствие реакции на атаку); $P_{\mathrm{II}}$ — вероятность ошибки II рода (ложное срабатывание).

Эксперименты проводились для КС, состоящей из 10 информационных ресурсов. Все СМБ сконфигурированы по принципу false positive, т.е. при обнаружении какого-либо подозрительного действия, которое нельзя достоверно идентифицировать, система относит его к классу потенциальных вторжений. В таком случае, как правило, $P_I \le P_{II}$.

Моделирование 75-ти дней работы КС показало результаты, приведенные на рис. 6 и 7.

На рис. 6 приведены графики зависимости вероятности корректной работы СМБ от времени. Как видно, при моделировании наихудшие результаты по корректности выявления атак показаны СМБ на основе алгоритма анализа вторжений статистического типа, а СМБ на основе нейросети и предложенного алгоритма по данной характеристике практически эквивалентны.

Далее проведены оценки затрат на реализацию СМБ перечисленных выше типов. При расчете затрат на построение СМБ учитываются следующие факторы:

$Z$ — общая величина затрат

$$Z = z_1 + z_2 + z_3 + z_4 + z_5 + z_6 + z_7 \ , \qquad (15)$$

где $z_1$ — затраты на аппаратную часть агентов сбора информации; $z_2$ — затраты на внедрение и поддержку ПО (средства сбора информации и проверки состояния КС); $z_3$ — затраты на СМБ; $z_4$ — затраты на оплату труда экспертов (7 у.е. /час); $z_5$ — затраты на оплату труда администратора безопасности (3 у.е. /час); $z_6$ — величина вычислительных затрат на СМБ КС (3 у.е. /час за каждые 10% ресурсов системы); $z_7$ — затраты из-за пропущенных атак (потеря, кража, искажение, недоступность информации и т.д., 50 у.е. /каждый ресурс).

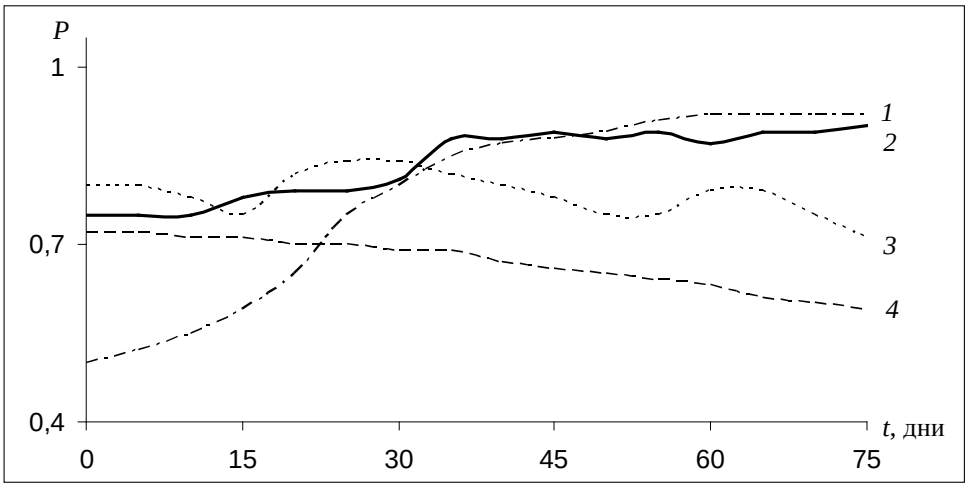


*Рис. 6.* Зависимости вероятности корректной работы от времени функционирования СМБ I (*4*), II (*3*), III (*1*), IV (*2*) типов

Значения факторов $z_1$, $z_2$, $z_3$ для всех СМБ приблизительно одинаковы.

Таким образом, при моделировании учитывались только факторы $z_4$, $z_5$, $z_6$, $z_7$.

На рис. 7 показаны текущие затраты на реализацию и поддержку функционирования СМБ за каждый день работы. Всплески на графике у всех СМБ отражают пропущенную на 15-й день успешную атаку, что требует настройки систем мониторинга для адекватной реакции в будущем. Максимумы на 60-й день связаны с аналогичным пропуском атаки СМБ I и II типов.

Для получения суммарной оценки затрат на реализацию СМБ за весь период наблюдений полученные кривые (рис. 7) интегрируются, т.е.

$$Z_\Sigma = \int_0^T z(t)dt \, , \qquad (16)$$

где $z(t)$ — затраты в определенный момент времени; $Z_\Sigma$ — суммарная стоимость затрат за весь период наблюдений $T$.

Как видно из рис. 7, суммарные затраты на реализацию СМБ на основе предложенного алгоритма оценки вероятности вторжений в КС оказываются наименьшими.

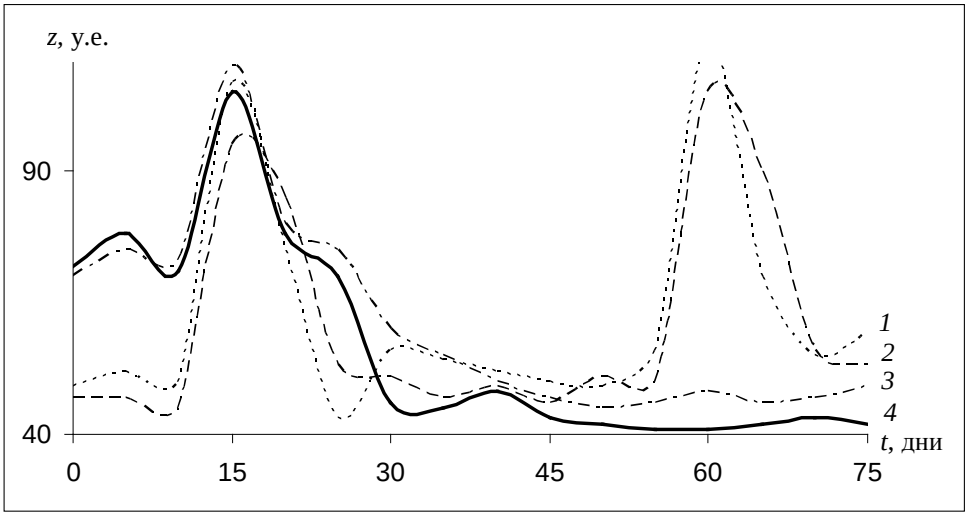


*Рис. 7.* Результаты экспериментальных исследований затрат на реализацию СМБ I (*2*), II (*1*), III (*3*), IV (*4*) типов

Также для сравнения характеристик СМБ целесообразно ввести показатель отношения качества работы СМБ (вероятности $p$ ее корректной работы) к уровню затрат $z$ на ее реализацию. Обозначим его $p/z$.

Как видно из рис. 8, СМБ на основе предложенного алгоритма оценки вероятности вторжений в КС имеет наилучший показатель отношения корректности ее функционирования к затратам на ее реализацию, что подтверждает эффективность разработанного алгоритма.

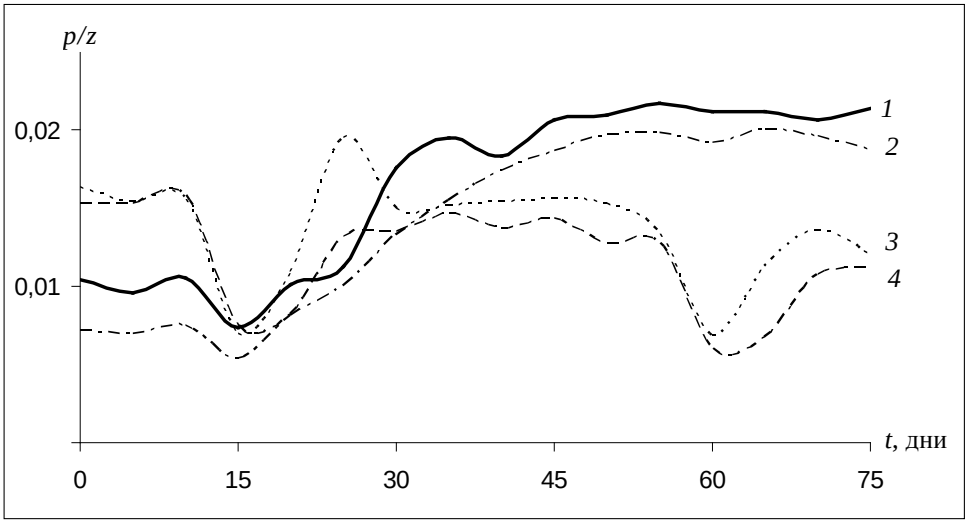


*Рис. 8.* Оценка показателя отношения корректности работы к уровню затрат на реализацию СМБ I (*4*), II (*3*), III (2), IV (*1*) типов

## ЗАКЛЮЧЕНИЕ

Построение качественных СМБ КС требует применения эффективных алгоритмов для анализа потенциальных атак злоумышленников в КС. Предложенный алгоритм формирования вероятностей вторжений в КС обеспечивает:

- повышение защищенности пользовательских и системных данных за счет выполнения прогнозирования действий злоумышленника и эмуляции уязвимостей и системных сведений;
- гибкую реакцию СМБ на действия нарушителя;
- ранжирование действий и целей субъектов по степеням их угроз безопасности КС;
- уменьшение объема анализируемой системой информации, что позволяет практически не снижать производительность КС.

Проведенный анализ основных параметров предложенного и аналогичных существующих алгоритмов подтвердил эффективность разработанного алгоритма, что обусловливается комплексным анализом в данном алгоритме целей действий легальных пользователей и злоумышленников в КС.

## ЛИТЕРАТУРА

1. *Галатенко В.А.* Основы информационной безопасности / Под ред. чл.-корр. РАН В.Б. Бетелина. — М.: ИНТУИР.RU, 2003. — 280 с.
2. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: Молгачева С.В., 2001. — 352 с.
3. *Bace R.* An Introduction to Intrusion Detection Assessment for System and Network // Security Management. — 1999. — № 7. — P. 167–180.
4. *Беляев А., Петренко С.* Системы обнаружения аномалий: новые идеи в защите информации // Экспресс-Электроника. — 2004. — № 2. — С. 57–71.
5. *Земсков И.А.* SIMCOSAR: Программный комплекс моделирования процесса мониторинга состояния информационного поля Интернет // Математические структуры и моделирование. — 2003. — № 11. — С.128–157.
6. *Система* функционального активного мониторинга FLAME / В.А. Васенин, В.В. Корнеев, М.Ю. Ландина, В.А. Роганов // Программирование. — 2003. — № 3. — С. 161–173.
7. *Вихорев С., Кобцев Р.* Как определить источники угроз? // Открытые системы. — 2002, № 7–8. — С. 37–49.

*Поступила 13.11.2006*