ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

УДК 004.89.021.056–047.58

Ю.Ю. Громов, В.М. Тютюнник

Модели оценки защищённости сетевых информационных систем от негативных внешних воздействий

Описана структура интеллектуальной информационной системы, предназначенной для защиты сетевой информационной системы от несанкционированных внешних воздействий с помощью различных средств парирования. Представлены условия устойчивого функционирования сетевой информационной системы. Сформулирована оптимизационная задача, которая заключается в необходимости минимизировать негативное внешнее воздействие на сетевую информационную систему с помощью средств парирования, поставляемых спроектированной интеллектуальной информационной системой. Эта задача разбивается на четыре подзадачи, для решения которых созданы аналитические модели, разработаны алгоритмы и показаны два примера аналитического решения задач оптимального распределения негативных внешних воздействий по элементам сетевой информационной системы без учёта и с учётом взаимного влияния элементов системы.

Ключевые слова: *интеллектуальная информационная система, сетевая информационная система, негативное внешнее воздействие, устойчивое функционирование систем, оценка защищённости, моделирование*

DOI: 10.36535/0548-0027-2021-10-2

ВВЕДЕНИЕ

Несколько лет назад мы начали исследования по построению общей теории информации и единой теории информационных систем. Проанализировав описанные в литературе меры для оценки количества информации, различные трактовки терминов «информация» и «данные», обобщив и описав свойства информации, нам удалось поначалу формализовать категорию «информация» и набор её свойств, представив их в тензорном виде. Введение в рассмотрение линейных пространств векторных функций принадлежности позволило обоснованно показать, что информация является тензорной величиной. Это дало возможность понять, что теория информации может быть разработана с помощью методов тензорного анализа и теории нечётких множеств, реализуя основные операции пересечения и объединения – *T*-норму и *T*-конорму (*S*-норму) соответственно [1-6].

Так как информация функционирует в информационных процессах и потоках, являющихся неотъемлемой составляющей информационных систем (ИС), которые в настоящее время большей частью представляются сетевыми, особое значение приобретает устойчивость функционирования сетевых информационных систем (СИС), причём в условиях, когда различные ресурсы этих систем подвергаются многочисленным несанкционированным внешним воздействиям (НВВ) [7-10].

СИС будет устойчиво функционировать, если соблюдаются следующие основные условия: 1) каждый информационный поток НВВ перекрыт соответствующим механизмом защиты, т. е. информационной технологией парирования НВВ; 2) надёжность (вероятность сопротивляемости) такой технологии стремится к единице, не позволяя преодолеть или обойти защиту; 3) размер ущерба, который может быть нанесён владельцу СИС в случае успеха НВВ, стремится к минимуму. Пока не известны стандартные методики реализации одновременно всех этих условий. Обычно уровень защищённости СИС определяется экспертами, которые лишь интуитивно могут учесть возможные синергетические взаимовлияния элементов СИС в процессе атаки НВВ. Однако имеются и автоматизированные системы анализа устойчивости функционирования (*security assessment systems*) или сканеры безопасности (*security scanners*).

ФОРМУЛИРОВКА ЗАДАЧИ И ПРОЕКТИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Учитывая три основные категории надёжного функционирования информационных систем (эффективность, безопасность, живучесть) [11], сконструируем структуру интеллектуальной ИС (рис. 1), которая является подсистемой СИС, анализирует совокупность данных и её состояния, делает вывод об уровне устойчивости её функционирования и вырабатывает рекомендации по повышению устойчивости.

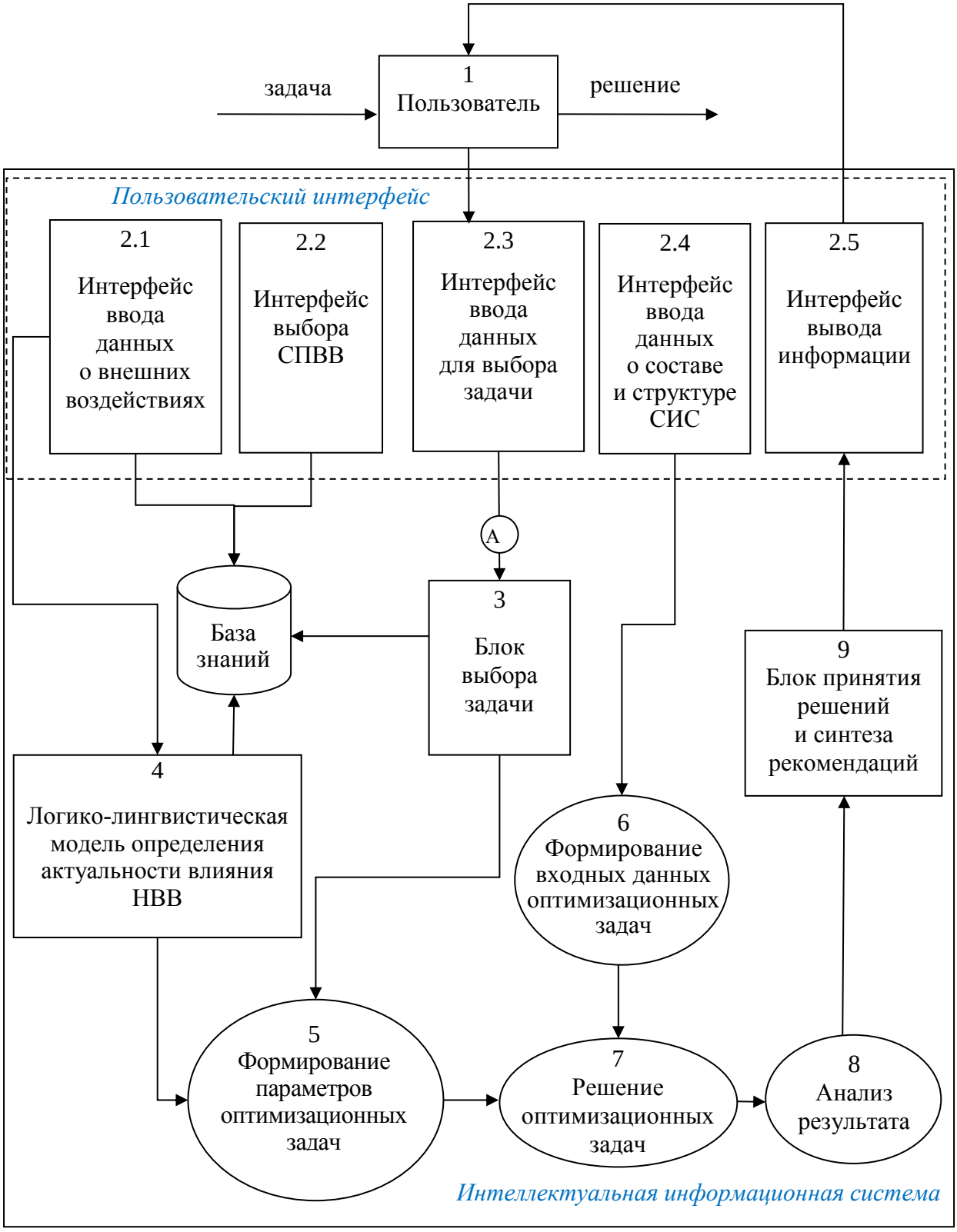

Рис. 1. Структура интеллектуальной информационной системы

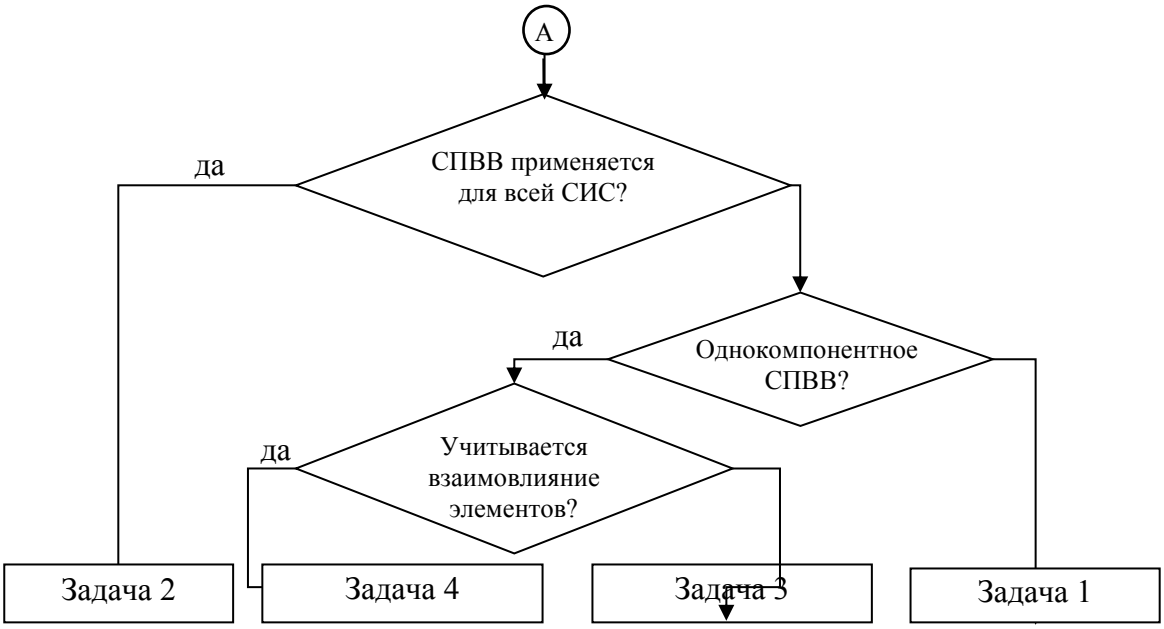

Рис. 2. Алгоритм выбора задачи распределения СПВВ в интеллектуальной ИС

Сформулируем оптимизационную задачу: имеется функционирующая СИС, на которую действуют несанкционированные внешние воздействия. Необходимо минимизировать воздействие НВВ с помощью средств парирования внешних воздействий (СПВВ), поставляемых интеллектуальной ИС. Эта задача разбивается на четыре подзадачи:

1) получить оптимальное количество компонентов одного типа СПВВ для каждого элемента СИС;

2) получить оптимальное количество СПВВ каждого типа для полной совокупности компонентов СИС;

3) получить набор СПВВ, который необходимо применить против каждого из известных наборов НВВ;

4) выбрать элемент СИС и конкретные СПВВ, которые необходимо применить против каждого из известного набора НВВ.

Интеллектуальная ИС (см. рис. 1) функционирует следующим образом. С помощью интерфейса ввода данных (блок 2) пользователь (1) задаёт состав защищаемой СИС: количество серверов, рабочих станций и информационных подсистем. Эти данные передаются в блок 3, который выбирает одну из четырёх подзадач на основе ответов на предложенные пользователю вопросы из базы знаний.

Выбор задачи осуществляется по следующему алгоритму.

Задача 1 решается в том случае, когда необходимо определить, какое количество компонентов одного СПВВ необходимо для каждого элемента защищаемой СИС. Здесь важно распределение СПВВ по элементам СИС, когда они устанавливаются на каждый элемент СИС, а СПВВ является многокомпонентным и требуется задать распределение его компонентов по элементам СИС.

Задача 2 решается в том случае, когда необходимо определить, какое количество СПВВ каждого типа необходимо для защиты всей СИС. Здесь важно использовать СПВВ, которые являются общими для всей СИС, либо не нужно учитывать распределение средств по конкретным элементам СИС.

Задача 3 решается в том случае, когда необходимо определить, какие СПВВ необходимо применять на каждом элементе защищаемой СИС, без учёта синергетического эффекта взаимовлияния элементов.

Задача 4 решается в том случае, когда необходимо определить, какие СПВВ необходимо применять на каком элементе защищаемой СИС с учётом синергетического эффекта взаимовлияния элементов. Здесь средства СППВ являются однокомпонентными.

Алгоритм выбора задачи (блок 3 на рис. 1) приведён на рис. 2.

Актуальность внешних воздействий определяется в блоке 4 (см. рис. 1) с помощью логико-лингвистической модели, используя правила нечёткого вывода, хранящиеся в базе знаний, и данные, полученные с помощью интерфейса ввода информации о внешних воздействиях (блок 2.1). Затем определяется полный набор СПВВ, в котором осуществляется выбор тех СПВВ, использование которых обеспечит максимальную устойчивость функционирования защищаемой СИС. Пользователь может самостоятельно скорректировать этот набор с помощью интерфейса выбора СПВВ (блок 2.2). Исходя из введённых пользователем данных варианта решаемой задачи, а также учитывая результаты деятельности блоков 4 или 5, в блоке 6 вычисляются параметры аналитической модели для решения оптимизационной задачи (блок 7). Затем данные из блоков 6 (параметры модели) и 7 (входные данные модели) подаются на вход блока 8, к аналитической модели. В результате работы аналитической модели получаются данные, которые далее анализируются в блоке 9 и подаются на вход блока 10, решающего следующие задачи: сформировать

рекомендации для повышения защищённости СИС; принять решение о допустимости практического использования СИС. В результате через блок 2.5 пользователь получает данные о количественной оценке устойчивости функционирования СИС и рекомендации по её повышению.

Решение задачи оптимального распределения негативных внешних воздействий по элементам сетевой информационной системы

Пусть дана СИС, состоящая из S элементов. На каждый элемент s_i воздействуют некоторые НВВ. Надо найти такие НВВ для каждого элемента СИС, при воздействии которых величина ущерба будет максимальной при заданных ограничениях.

Математическая постановка задачи: требуется найти оптимальный вектор $X = \{x_i, i = \overline{1,S}\}$ распределения НВВ по элементам СИС, обусловливающий максимум функции ущерба

$$F(X) = \sum_{i=1}^{S} A_i \left(1 - q_i^{x_i}\right) \to \max_{x_i}, \qquad (1)$$

при ограничении на его компоненты

$$\sum_{i=1}^{S} x_i \le N, \qquad (2)$$

и при дополнительных условиях

$$x_i \in \{0,1,..,N\}, \qquad (3)$$

$$0 \le (p_i = 1 - q_i) \le 1, \qquad (4)$$

где:

A_i – относительная важность i-го элемента СИС;

p_i – вероятность того, что НВВ выведет из строя i-й элемент СИС;

q_i – вероятность того, что НВВ не выведет из строя i-й элемент СИС;

$q_i^{x_i}$ – вероятность того, что ни одно из x_i НВВ не выведет из строя i-й элемент СИС;

$(1 - q_i^{x_i})$ – вероятность того, что хотя бы одно из x_i НВВ выведет из строя i-й элемент СИС;

N – количество НВВ, равных по эффективности;

S – количество элементов СИС.

Поставленная задача (1 – 4) является задачей целочисленного программирования, поскольку на элементы искомого вектора $X = \{x_i, i = \overline{1,S}\}$ наложено ограничение (3). Представим критерий оптимизации (1) следующим образом:

$$F(x) = \sum_{i=1}^{S} F_i(x_i) = \sum_{i=1}^{S} A_i \left(1 - q_i^{x_i}\right). \qquad (5)$$

Преобразуем $F_i(x_i)$ к следующему виду:

$$F_i(x_i) = A_i \left(1 - q_i^{x_i}\right) = A_i p_i + A_i q_i\, p_i + A_i q_i^{x_i - 1} p_i = \\ = \Delta_{1k}^{+} + \Delta_{2k}^{+} + ... + \Delta_{x_i i}^{+} = \sum_{k=1}^{x_i} \Delta_{ki}^{+}. \qquad (6)$$

Отсюда следует, что критерий оптимизации состоит из суммы критериев величины ущерба по каждому элементу СИС, зависящих от распределения НВВ на каждом элементе СИС. Введём обозначение $\Delta_{ik}^{+} = A_i q_i^{k-1} \varepsilon_i$. Таким образом, $F_i(x_i)$ составляет убывающую последовательность приращений Δ_{ik}^{+}.

На каждом этапе будем распределять СПВВ последовательно – по одному на каждый элемент СИС. Величину ущерба на t-м этапе вычислим по формуле

$$F_t^{+} = \sum_{i=1}^{S} A_i \left(1 - q_i^{x_i^{(t)}}\right),$$

где вектор

$$X^{(t)} = \{x_i^{(t)}, i = \overline{1,S}, t = \overline{0,N}\}$$

является искомым вектором на t-м этапе. Очевидно, что $X^{(0)} = \{0,...,0\}$, поскольку на начальном этапе ни одно средство не соотнесено ни с одним элементом СИС.

Пусть на некотором t-м этапе на l-й элемент распределено t-е средство. Тогда разность количественных оценок величин ущерба СИС на t-м и $(t-1)$-м этапах можно вычислить:

$$\Delta_l^{+} = F_t^{+} - F_{t-1}^{+} = \sum_{i=1}^{S} A_i \left(1 - q_i^{x_i^{(t)}}\right) - . \\ - \sum_{i=1}^{S} A_i \left(1 - q_i^{x_i^{(t-1)}}\right) = \sum_{i=1}^{S} A_i \left(q_i^{x_i^{(t-1)}} - q_i^{x_i^{(t)}}\right)$$

Поскольку лишь одно средство распределяется за один этап, векторы $X^{(t)}$ и $X^{(t-1)}$ отличаются лишь одним l-м элементом, и $x_l^{(t)} - x_l^{(t-1)} = 1$. Отсюда выражение разности количественных оценок величин ущерба СИС на t-м и $(t-1)$-м этапах примет вид: $\Delta_l^{+} = F_t^{+} - F_{t-1}^{+} = A_l \cdot (1 - q_l) = A_l \cdot p_l$. Поскольку A_l – положительная константа, а p_l – вероятность, то $\Delta_l^{+} \ge 0$.

Составим алгоритм решения поставленной задачи на основе проведённых рассуждений.

1. Вычислить для каждого $l=\overline{1,S}$ приращение Δ_l^+ по формуле $\Delta_l^+ = A_l\ p_l,\quad l=\overline{1,S}$.

2. Назначить единицы НВВ на $i=l_t$ объект согласно условию $\Delta_{l_t}^+ = \max\limits_{1\le l\le S}\Delta_l^+$.

3. Вычислить текущее значение вектора X по условиям $x_i^{(t)} = \begin{cases} x_i^{(t-1)}, если\ i\ne l_t \\ x_i^{(t-1)}+1, если\ i=l_t \end{cases}$.

Здесь начальное значение $x_i^{(0)}=0, i=\overline{1,S}$.

4. Вычислить текущее значение целевой функции

$$F_t^+ = F_{t-1}^+ + \Delta_{l_t}^+, F_0^+ = 0, t=t+1.$$

5. Проверить соблюдение условия $t\le N$; если оно соблюдается, то перейти к пункту 6, если не соблюдается – то к пункту 7.

6. Пересчитать компоненты текущего вектора $\left(\Delta_l^+\right)^{(t)}$ по условию

$$\Delta^+{}_l = \begin{cases} \Delta_l^+, если\ l\ne l_t \\ \Delta_l^+\cdot p_i, если\ l=l_t \end{cases}.$$

Перейти к пункту 2.

7. Вывести результаты расчётов в виде

$$F(x_0)=F_N^+, x_i = x_i^{(N)}.$$

Остальные три задачи решаются аналогично. Особый интерес представляет учёт взаимного влияния элементов.

Решение задачи оптимального распределения негативных внешних воздействий по элементам сетевой информационной системы с учётом взаимного влияния элементов

Рассмотрим СИС, состоящую из *S* элементов (рабочих станций и серверов), и на которую действует набор из *M* типов НВВ. Все элементы СИС взаимосвязаны, поэтому потеря работоспособности одного элемента влияет на работоспособность других элементов. Количество НВВ каждого типа равно N_j, $j=\overline{1,M}$. Необходимо так сгруппировать НВВ и распределить их по элементам СИС, чтобы функция ущерба достигла максимального значения.

Математическая постановка задачи: требуется найти вектор $X=\left\{x_{ji}, i=\overline{1,S}, j=\overline{1,M}\right\}$ оптимального распределения НВВ по взаимосвязанным элементам СИС, чтобы функция ущерба (7) достигла максимального значения.

$$F(X)=\sum_{i=1}^{S} A_i\cdot\left(1-\prod_{y=1}^{S}\left[1-\alpha_{iy}\left(1-\prod_{j=1}^{M} q_{ji}^{x_{ji}}\right)\right]\right)\to\max_{x_{ji}}, \quad (7)$$

при ограничении на его компоненты

$$\sum_{i=1}^{S} x_{ji}\le N,\quad j=\overline{1,M}, \quad (8)$$

и дополнительных условиях:

$$x_{ji}\in\{0,1\},\ \sum_{i=1}^{S}\sum_{j=1}^{M} x_{ji}=N,\ 0\le(p_{ji}=1-q_{ji})\le 1,$$

$$A_i\ge 0; i=\overline{1,S}; j=\overline{1,M},\ \ 0\le\alpha_{iy}\le 1, y=\overline{1,S}.$$

Здесь:

A_i – относительная важность *i*-го элемента СИС;

M – количество типов НВВ;

N – общее количество НВВ разных типов, которые действуют на СИС;

S – количество элементов СИС;

α_{iy} – коэффициент взаимовлияния элементов СИС, вероятность того, что выход из строя *y*-того элемента повлечёт за собой сбои в работе *i*-го элемента (0 – элементы не взаимодействуют, 1 – однозначный выход из строя элемента);

p_{ji} – вероятность того, что НВВ *j*-го типа выведет из строя *i*-й элемент СИС;

q_{ji} – вероятность того, что НВВ *j*-го типа не выведет из строя *i*-й элемент СИС;

$q_{ji}^{x_{ji}}$ – вероятность того, что ни одно из x_{ji} НВВ *j*-го типа не выведет из строя *i*-й элемент СИС;

$\prod\limits_{j=1}^{M} q_{ji}^{x_{ji}}$ – вероятность того, что ни одно НВВ не выведет из строя *i*-й элемент СИС;

$1-\prod\limits_{j=1}^{M} q_{ji}^{x_j}$ – вероятность того, что хотя бы одно НВВ выведет из строя *i*-й элемент СИС;

$\alpha_{iy}\left(1-\prod\limits_{j=1}^{M} q_{ji}^{x_{ji}}\right)$ – вероятность того, что одновременно и НВВ, и другой элемент выведут из строя *i*-й элемент СИС;

$[1-\alpha_{iy}\left(1-\prod\limits_{j=1}^{M} q_{ji}^{x_{ji}}\right)]$ – вероятность того, что хотя бы одно из НВВ или сломанный *y*-й элемент не выведет из строя *i*-й элемент СИС.

Поставленная задача также является задачей целочисленного программирования.

По формуле (7) видно, что если все элементы вектора *X* являются нулями, то $F_0=0$. Пусть выбран E_t элемент СИС для *t*-го этапа. Необходимо найти такое l_t-е НВВ, чтобы разность величин ущерба СИС на *t*-м и (*t*-1)-м этапах вычислялась по формуле:

$$\Delta^+_{lE} = F^+_t - F^+_{t-1} = \sum_{i=1}^{S} A_i \cdot \left(1 - \prod_{y=1}^{S}\left[1 - \alpha_{iy}\left(1 - \prod_{j=1}^{M} q_{ji}^{x^t_{ji}}\right)\right]\right) -$$

$$- \sum_{i=1}^{S} A_i \cdot \left(1 - \prod_{y=1}^{S}\left[1 - \alpha_{iy}\left(1 - \prod_{j=1}^{M} q_{ji}^{x^{t-1}_{ji}}\right)\right]\right) =$$

$$= \sum_{i=1}^{S} A_i \cdot \left(\prod_{y=1}^{S}\left[1 - \alpha_{iy}\left(1 - \prod_{j=1}^{M} q_{ji}^{x^{t-1}_{ji}}\right)\right] - \prod_{y=1}^{S}\left[1 - \alpha_{iy}\left(1 - \prod_{j=1}^{M} q_{ji}^{x^{t}_{ji}}\right)\right]\right) =$$

$$= \sum_{i=1}^{S} A_i \cdot \left(\prod_{y=1}^{S}\left[\alpha_{iy}\prod_{j=1}^{M} q_{ji}^{x^{t-1}_{ji}} - \alpha_{iy} + 1\right] - \prod_{y=1}^{S}\left[\alpha_{iy}\prod_{j=1}^{M} q_{ji}^{x^{t}_{ji}} - \alpha_{iy} + 1\right]\right) =$$

$$= A_{E_t} \cdot \left(\prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y}\prod_{j=1}^{M} q_{jE_t}^{x^{t-1}_{jE_t}} - \alpha_{E_t y} + 1\right] - \prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y}\prod_{j=1}^{M} q_{jE_t}^{x^{t}_{jE_t}} - \alpha_{E_t y} + 1\right]\right).$$

Введём обозначение $c_i^t = \prod_{j=1}^{M} q_{ji}^{x^t_{ji}}$, тогда выражение упростится:

$$\Delta^+_{E_t l_t} = A_{E_t} \cdot \left(\prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y} c_{E_t}^{t-1} - \alpha_{E_t y} + 1\right] - \prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y} c_{E_t}^{t-1} \cdot q_{l_t E_t} - \alpha_{E_t y} + 1\right]\right).$$

Для решения задачи (7) предлагается следующий алгоритм:

1. Определить начальные переменные:

$$t = 1; c_i^{(0)} = 1, i = \overline{1,S};\ x_{ji}^{(0)} = 0, j = \overline{1,M};\ F_0^+ = 0.$$

2. Вычислить вектор приращений величин ущерба СИС:

$$\Delta^+_{E_t l_t} = A_{E_t} \cdot \left(\prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y} \cdot c_{E_t}^{t-1} - \alpha_{E_t y} + 1\right] - \prod_{\substack{y=1 \\ y \neq E_t}}^{S}\left[\alpha_{E_t y} \cdot c_{E_t}^{t-1} \cdot q_{l_t E_t} - \alpha_{E_t y} + 1\right]\right)$$

.

3. Выбрать тип средства, обеспечивающий максимальный ущерб на данном этапе:

$$\Delta^+_{l_t E_t} = \max_{\substack{1 \le l \le M \\ 1 \le E \le S}} \Delta^+_{lE}.$$

4. Отметить выбор в векторе X:

$$x_{ji}^{(t)} = \begin{cases} x_{ji}^{(t-1)}, j \neq l_t, i \neq E_t \\ x_{ji}^{(t-1)} + 1, j = l_t, i = E_t \end{cases}.$$

5. Пересчитать величины c_{E_t} по формуле:

$$c_{E_t}^{(t)} = c_{E_t}^{(t-1)} \cdot q_{l_t E_t}, i = \overline{1,S}.$$

6. Получить значение ущерба на данном этапе:

$$F_t^+ = F_{t-1}^+ + \Delta^+_{l_t E_t}.$$

7. Перейти к следующему этапу: $t = t + 1$.

8. Если $t \le N$, то перейти к пункту 2, если нет, то перейти к пункту 9.

9. Вывести результат X и максимальный ущерб СИС F_t^+.

Пример реализации описанных моделей

Имеется сетевая информационная система, состоящая из трёх (S = 3) элементов (две рабочих станции и один сервер), обладающих заданной, соответственно, важностью A = (20, 50, 30), причём $\sum_{i=1}^{S} A_i = 100\%$. Пусть на СИС действуют M = 4 типов НВВ: 1) вирусы; 2) сбой в работе оборудования; 3) несанкционированный доступ злоумышленника; 4) сетевые черви. Пусть количество НВВ каждого типа N_j равно двум, и пусть на каждый элемент СИС может оказывать воздействие НВВ одного типа только один раз, т. е. $x_{ji} \in \{0,1\}$. Вероятности того, что НВВ j-го типа не выведет из строя i-й элемент СИС, представлены матрицей Q:

$$Q = \begin{pmatrix} 0.5 & 0.2 & 0.3 & 0.6 \\ 0.3 & 0.4 & 0.2 & 0.3 \\ 0.5 & 0.2 & 0.3 & 0.4 \end{pmatrix}.$$

Требуется выбрать для каждого из элементов S = 3 такой набор НВВ средств парирования, чтобы величина ущерба всей системы при этих воздействиях была максимальной. В таблице представлены этапы расчёта и значения ущерба на каждом этапе, а также результирующий вектор X.

Этапы расчёта значения ущерба

Этапы, t	$C_i^{(t)}, i = \overline{1,S}, j = \overline{1,M}$ для каждого из трёх элементов:			$\Delta^+_{E_t l_t}, E = \overline{1,S}, l = \overline{1,M}$				F_t^+
1	20	50	30	10	16	14	8	40
				35	30	**40**	35	
				15	24	21	18	
2	20	10	30	10	16	14	8	64
				7	6	8	7	
				15	**24**	21	18	
3	20	10	6	10	**16**	14	8	80
				7	6	8	7	
				3	4,8	4,2	3,6	
4	4	10	6	2	3,2	2,8	1,6	87
				7	6	8	7	
				3	4,8	**4,2**	3,6	

Этапы, t	$C_i^{(t)}, i=\overline{1,S}, j=\overline{1,M}$ для каждого из трёх элементов:			$\Delta^+_{E_t l_t}, E=\overline{1,S}, l=\overline{1,M}$				F_t^+
5	4	3	6	2	3,2	2,8	1,6	91,2
				2,1	1,8	2,4	2,1	
				3	4,8	**4,2**	3,6	
6	4	3	1.8	2	3,2	2,8	1,6	93,3
				2,1	1,8	2,4	**2,1**	
				0,9	1,44	1,26	1,08	
7	4	0.9	1.8	**2**	3,2	2,8	1,6	95,3
				0,63	0,54	0,72	0,63	
				0,9	1,44	1,26	1,08	
8	2	0.9	1.8	1	1,6	1,4	0,8	96,38
				0,63	0,54	0,72	0,63	
				0,9	1,44	1,26	**1,08**	
	X =	1	1	0	0			96,38
		1	0	1	1			
		0	1	1	1			

Результат выбора наилучшего приращения величин ущерба F_t^+ выделен на каждом этапе. Таким образом видно, что обеспечение максимального ущерба рассматриваемой СИС достигается воздействием: 1) вирусов на 1-й и 2-й элементы СИС; 2) сбоя в работе оборудования на 1-й и 3-й элементs СИС; 3) несанкционированного доступа злоумышленника на 2-й и 3-й элементы СИС; 4) сетевых червей на 2-й и 3-й элементы СИС.

ЗАКЛЮЧЕНИЕ

Представленная в настоящей статье интеллектуальная информационная система надёжно защищает сетевую информационную систему от несанкционированных внешних воздействий с помощью различных средств парирования. Сформулированы условия устойчивого функционирования сетевой информационной системы. Оптимизационная задача, состоящая в необходимости минимизировать несанкционированное внешнее воздействие на сетевую информационную систему с помощью средств парирования, поставляемых спроектированной интеллектуальной информационной системой, разбивается на четыре подзадачи, для решения которых созданы аналитические модели, разработаны алгоритмы и показаны два примера аналитического решения задач оптимального распределения негативных внешних воздействий по элементам сетевой информационной системы без учёта и с учётом взаимного влияния её элементов. Расчёты по этим моделям позволят выбирать средства парирования негативного внешнего воздействия и обеспечивать защиту сетевой информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Gromov Yu.Yu., Tyutyunnik V.M. Materials for the Information Theory Elaboration. 1. Information Quantity and Quality Measures // Journal of International Scientific Publications: Materials, Methods & Technologies. – 2011. – Vol. 5, Part 1. – P. 230-241.
2. Громов Ю.Ю., Тютюнник В.М. Материалы к разработке теории информации. 1. Меры количества и качества информации // Фундаментальные исследования. – 2011. – №8, ч. 2. – С. 347-355.
3. Gromov Yu.Yu., Tyutyunnik V.M., Minin Yu.V. Materials to the Theory of Information Elaboration. 2. Information as Tensor Quantity and Information System Modeling // International Journal of Research in Engineering, IT and Social Sciences. – 2018. – Vol. 8, Issue 6. – P. 1-14.
4. Gromov Yu.Yu., Tyutyunnik V.M., Minin Yu.V. Materials to the theory of information elaboration. 3. Information systems modeling // Материалы XVIII Международной научной конференции «Формирование профессионала в условиях региона: новые подходы» (г. Тамбов, 7-8 июня 2018 г.) / под ред. проф. В.М. Тютюнника, проф. В.А.Зернова. – Тамбов; Москва; Санкт-Петербург; Баку; Вена; Гамбург; Стокгольм: Изд-во МИНЦ «Нобелистика», 2018. – С. 87-106.
5. Громов Ю.Ю., Тютюнник В.М., Минин Ю.В. Материалы к разработке теории информации. 4. Тензорное измерение информации для моделирования информационной системы // Информационные системы и процессы: сб. науч. тр. / под ред. проф. В.М. Тютюнника. – Тамбов; Москва; Санкт-Петербург; Баку; Вена; Гамбург; Стокгольм: Изд-во МИНЦ «Нобелистика», 2018. – Вып.17. – С.7-28.
6. Тютюнник В.М. , Громов Ю.Ю., Александров Е.Ю. Аналитические модели парирования негативных внешних воздействий на сетевую информационную систему // Научно-техническая информация. Сер. 2. – 2020. – № 9. – С.15-20. DOI: 10.36535/0548-0027-2020-09-03;
7. Tyutyunnik V.M., Gromov Yu.Yu., Aleksandrov E.Yu. Analytical models of negative

external influences vaporizing on the network information system // Automatic Documentation and Mathematical Linguistics. – 2020. – Vol. 54, № 5. – P. 250-254. DOI: 10.3103/S0005105520050040.
8. Liang X., Xiao Ya. Game Theory for Network Security // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, № 1. – P. 472-486.
9. Gupta J., Ulmer A., Chaturvedi A., Chi J. Matching information security vulnerabilities to organizational security profiles: A genetic algorithm approach // *Decision Support Systems.* – 2006. – Vol. 41, №3. – P. 592-603.
10. Hashemi S.M., He J., Ebrahimi Basabi A. Multi-objective optimization for computer security and privacy // International Journal of Network Security. – 2017. – Vol. 19, № 3. – P. 394-405.
11. Dewri R., Poolsappasit N., Ray I., Whitley D. Optimal security hardening using multi-objective optimization on attack tree models of networks // Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07). – 2007. – P.204-213.
12. Firesmith D.G. Common Concepts Underlying Safety, Security, and Survivability Engineering. – Pittsburgh, PA: Carnegie Mellon University. – 2003. – 62 p.

Материал поступил в редакцию 30.08.21.

Сведения об авторах

ГРОМОВ Юрий Юрьевич – доктор технических наук, профессор, Тамбовский государственный технический университет, директор Института автоматики и информационных технологий
e-mail: gromovtambov@yandex.ru

ТЮТЮННИК Вячеслав Михайлович – доктор технических наук, профессор, профессор кафедры конструирования радиоэлектронных и микропроцессорных систем Тамбовского государственного технического университета; генеральный директор Международного Информационного Нобелевского Центра (МИНЦ)
e-mail: vmtyutyunnik@gmail.com