ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

И.В. Атласов,
доктор физико-математических наук, профессор

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СКУПКИ БАНКОВСКИХ КАРТ ЗЛОУМЫШЛЕННИКОМ

A MATHEMATICAL MODEL OF BUYING UP BANK CARDS BY AN INTRUDER

Рассмотрена математическая модель оценки вреда, причиненного клиентам банка злоумышленником, который покупает ворованные данные с банковских карт. Изучен вопрос о выборе оптимальной стратегии покупки данных, при выборе которой клиентам банка будет нанесен максимальный ущерб.

The mathematical model of assessing harm to customers of the bank by an attacker who buys the stolen data from credit cards is considered. The question of choosing the optimal strategy of buying the data, the choice of which bank customers will suffer the maximum damage is examined.

1. Постановка задачи оптимального уравнения для стохастического дифференциального уравнения, управляющего работой злоумышленника

На сегодняшний день в банковской сфере актуальной является задача уберечь капиталы клиентов, находящиеся на пластиковых банковских картах. Очень много совершается попыток снять деньги с этих карточек, и большая часть попыток удачна. Поэтому для банка крайне важна оценка ущерба, причиненного злоумышленниками, с целью оборудования банкоматов и банковских карт адекватными мерами защиты от похищения информации, находящейся на банковских картах и в банкоматах.

В настоящее время практически на всех предприятиях работники получают свою заработную плату через банковские карточки. Как правило, эти банковские карточки слабо защищены, при несанкционированном доступе к этим карточкам относительно легко прочитать надпись на магнитной карте и несложно вычислить четырехзначный код.

Подавляющее большинство людей получают относительно небольшую сумму достаточно регулярно, в том смысле, что на карточке всегда находится более или менее постоянная сумма. В дальнейшем эти карточки мы будем называть карточками первого вида.

С другой стороны, есть работники, имеющие достаточно высокий доход и тоже получающие деньги по банковским карточкам, которые защищены несколько лучше. То есть сложнее считывать код, данные на магнитной полосе. Также это означает, что при несанкционированном доступе к этим карточкам можно снять и достаточно большую сумму, можно снять и меньшую, чем на карточках первого вида, и в крайнем случае можно и ничего с карточки не получить. В дальнейшем эти карточки мы будем называть карточками второго вида.

Предположим, что кто-то занимается воровством данных банковских карт и кодов к ним. Затем этот человек изготавливает поддельные банковские карты и продает данные злоумышленнику, деятельность которого мы и будем рассматривать.

Деятельность нашего злоумышленника состоит в покупке фальшивых банковских карт, снятии с них денежных средств, покупке на эти денежные средства новых банковских карт, снова снятии с них денежных средств и так далее. Предположим, что этот процесс непрерывный, но не мгновенный, и что за время деятельности злоумышленника остановить его преступную деятельность практически невозможно.

Пусть у злоумышленника стоит задача на конкретный момент времени, выбранный произвольно, получить максимальную прибыль. Самый простой вариант решения этой задачи — купить на все деньги банковские карточки первого вида и получать более или менее гарантированный доход, пропорциональный вложенным деньгам и потраченному времени (время будем измерять в днях) с коэффициентом пропорциональности b. То есть, имея в некоторый момент времени t количество X_t денежных знаков, к моменту времени $t+\Delta t$ мы будем иметь $X_{t+\Delta t} = X_t\left(1+b\Delta t\right)$ денежных знаков. Последняя формула приобретает вид

$$\begin{aligned} X_{t+\Delta t} - X_t &= bX_t\Delta t \\ \frac{X_{t+\Delta t} - X_t}{\Delta t} &= bX_t \end{aligned} \qquad (1)$$

и, перейдя к производной к пределу при $\Delta t \to 0$

$$\lim_{\Delta t\to 0}\frac{X_{t+\Delta t} - X_t}{\Delta t} = X_t^{(*)},$$

получим обыкновенное дифференциальное уравнение

$$dX_t = bX_t dt, \quad X_t^{(*)} = bX_t, \qquad (2)$$

решение которого хорошо известно и имеет вид

$$X_t = X_0 \exp\left(bt\right). \qquad (3)$$

Используя это выражение, подсчитаем, сколько необходимо времени, чтобы удвоить капитал, например для b=0,2. Выполняя несложные вычисления, получим

$2X_0=X_0exp(0,2t)$, $t=5e^2\approx 36,45$,

то есть необходимо около 37 дней, чтобы удвоить капитал, что может не удовлетворить владельца капитала.

Например, при b=0,8 легко подсчитать, что необходимо около $t \approx 9$ дней, что более приемлемо. К сожалению, таких доходов без риска получить невозможно. При покупке банковских карт второго вида нельзя указать единый коэффициент b, для которо-

го была бы справедлива формула (1). Этот коэффициент будет меняться в зависимости от времени. То есть вместо формулы $X_{t+\Delta t} - X_t = aX_t\Delta t$ получается формула

$$X_{t+\Delta t} - X_t = aX_t\Delta t + W_t\Delta t X_t, \quad (4)$$

где a — коэффициент пропорциональности ожидаемой прибыли, а W_t — некоторый случайный процесс. Обозначим $\Delta V_t = V_{t+\Delta t} - V_t = W_t\Delta t$ и потребуем выполнения для процесса V_t некоторых условий:

• Процесс V_t имеет независимые приращения, то есть величины V_{t_1}, $V_{t_2} - V_{t_1}$, $V_{t_k} - V_{t_{k-1}}$ независимы для всех $0, t_1, t_2, \ldots, t_k$.

• $V_{t_2} - V_{t_1}$ является стационарным процессом, то есть распределения процессов V_t и V_{t+h} для всех h совпадают.

• Математическое ожидание $E(V_t) = 0$ для всех $t > 0$.

• Процесс V_t имеет непрерывные траектории.

Рассмотрим эти условия подробнее. Первое условие означает, что прибыль, получаемая в данный момент, не зависит от прибыли, полученной ранее. Второе условие означает, что деньги можно вкладывать в любое время, ожидание прибыли от этого не изменится. Третье условие означает, что ожидание прибыли должно быть равно a. Четвертое условие говорит о возможности применения математического аппарата. То есть все условия естественны и вытекают из условия задачи. Здесь хотелось бы отметить, что единственным процессом, удовлетворяющим этим условиям, является броуновское движение B_t [1]. То есть формула (4) приобретает вид

$$X_{t+\Delta t} - X_t = aX_t\Delta t + \alpha\Delta B_t X_t, \quad (5)$$

где α — некоторая нормирующая константа и, естественно, $a \gg b$, то есть рискованный способ увеличить капитал всегда ожидает большего дохода. К счастью, эта задача также формализована и последняя формула эквивалентна стохастическому дифференциальному уравнению

$$X_t^{(*)} = aX_t + \alpha X_t W_t, \quad (6)$$

где символом W_t обозначен «белый шум». В свою очередь, можно считать, что это уравнение эквивалентно одному из уравнений

$$dX_t = aX_t dt + \alpha X_t dB_t, \quad X_t = X_0 + a\int_0^t X_s ds + \alpha\int_0^t X_s dB_s, \quad (7)$$

$$dX_t = aX_t dt + \alpha X_t \circ dB_t, \quad X_t = X_0 + a\int_0^t X_s ds + \alpha\int_0^t X_s \circ dB_s, \quad (8)$$

где интегралы $\int_0^t X_s dB_s$ и $\int_0^t X_s \circ dB_s$ являются интегралами Ито и Стратоновича соответственно. Могут быть и другие варианты интеграла, но принципиальной разницы эти интегралы не несут. Используя формулу Ито, можно найти решения этих дифференциальных уравнений. Функция $X_t = X_0 \exp\left(\left(a - \frac{1}{2}\alpha^2\right) + \alpha B_t\right)$ является решением уравнения (7). Функция $\overline{X}_t = X_0 \exp(at + \alpha B_t)$ является решением уравнения (8). Перейдем к вопросу о

выборе решения. Естественно предположить, что X_0 и B_t — независимые случайные величины. При этом условии математические ожидания случайных величин X_t и $\overline{X}_t$

$$E\left(X_t\right) = E\left(X_0\right)\exp\left(at\right), \tag{9}$$

$$E\left(\overline{X}_t\right) = E\left(X_0\right)\exp\left(\left(a+\frac{1}{2}\alpha^2\right)t\right). \tag{10}$$

Видно, что средний доход должен вычисляться по формуле (9), то есть интеграл Ито (7) нам подходит больше. Более того, интеграл Ито предпочтителен тем, что при своем построении не использует «информацию из будущего».

Итак, у владельца капитала есть выбор: либо вложить деньги в банковские карточки первого вида, либо вложить деньги в банковские карточки второго вида. Но он может действовать осторожнее, то есть часть денег вложить в банковские карточки первого вида и часть вложить в банковские карточки второго вида, причем делать это в любой момент времени.

Составим на этот случай дифференциальное уравнение. Для некоторой измеримой функции $0 \le u_t \le 1$ умножим уравнение (2) на u_t, а уравнение (7) на $1-u_t$ и получим уравнение

$$\begin{aligned} dX_t &= u_t dX_t + \left(1-u_t\right)dX_t = \left(1-u_t\right)bX_t dt + u_t\left(aX_t dt + \alpha X_t dB_t\right) \\ dX_t &= X_t\left(u_t a + b\left(1-u_t\right)\right)dt + \alpha u_t X_t dB_t \end{aligned} \tag{11}$$

Назовем это уравнение стохастическим дифференциальным уравнением, управляющим работой злоумышленника.

2. Существование и единственность решения стохастического дифференциального уравнения

Для уравнения (11) весьма актуальным является вопрос о существовании и единственности решения. Для этого введем новые обозначения и рассмотрим более подробно броуновское движение.

Пусть $0 \le s \le t_1 \le t_2 \le \ldots \le t_n$ и $F_k \in R^n$ — борелевские множества. Обозначим

$$P^x\left[w : X_{t_1}\left(w\right) \in F_1, \ldots, X_{t_n}\left(w\right) \in F_n\right] =$$

$$= \int\limits_{F_1 \times \ldots \times F_n} p\left(t_1, x, x_1\right) p\left(t_2 - t_1, x_1, x_2\right) \ldots p\left(t_n - t_{n-1}, x_{n-1}, x_n\right) dx_1 \ldots dx_n ,$$

где $x_i = \left(x_i^1, \ldots, x_i^n\right)$, $x = \left(x^1, \ldots, x^n\right)$ и

$$p\left(t, x_i, x_j\right) = \left(2\pi t\right)^{-\frac{1}{2}} \exp\left(-\frac{\sum\limits_{k=1}^{n}\left(x_i^k - x_j^k\right)^2}{2t}\right), \quad p\left(0, x_i, x_j\right) = \delta_{x_i}\left(x_j\right),$$

где $\delta_{x_i}\left(x_j\right)$ — так называемая обобщенная функция δ. Очевидно, $P^x\left(B_0 = x\right) = 1$.

Также символом E^x будем обозначать математическое ожидание случайной величины относительно вероятностной меры P^x.

Определение 1. *Обозначим символом $\mathfrak{F} = \mathfrak{F}^{(n)}$ наименьшую σ-алгебру, содержащую все множества вида $\left\{w : B_{t_1}\left(w\right) \in F_1, B_{t_2}\left(w\right) \in F_2, \ldots, B_{t_n}\left(w\right) \in F_n\right\}$ для всех борелевских на R^n множеств F_i.*

Определение 2. *Обозначим символом* $\mathfrak{F}_t = \mathfrak{F}_t^{(n)}$ *наименьшую* σ*-алгебру, содержащую все множества вида* $\left\{w : B_{t_1}(w) \in F_1, B_{t_2}(w) \in F_2, \ldots, B_{t_n}(w) \in F_n\right\}$ *для всех* $t_i \le t$, $n \in N$ *и всех борелевских на* R^n *множеств* F_i.

Заметим, что $\mathfrak{F}_s \subset \mathfrak{F}_t$ при $s < t$, то есть семейство $\mathfrak{F}_t$ является возрастающим.

Определение 3. *Обозначим символом* $\mathfrak{L} = \mathfrak{L}^{(n)}(S,T)$ *класс функций*

$f(t,x) : [0,\infty) \times \Omega \to R^n$ *таких, что выполняются следующие условия:*

• функция $(t,w) \to f(t,w)$ является $\mathfrak{P} \times \mathfrak{I}$ измеримой, где $\mathfrak{B}$ означает борелевскую σ-алгебру на $[0,\infty)$;

• функция $f(t,w)$ является $\mathfrak{F}_t$ согласованной;

• $P^x\left[w : \int_S^T f^2(t,w)\,dt < \infty\right] = 1$.

Определение 4. *Также символом* $\mathfrak{L} = \mathfrak{L}^{(m\times n)}(S,T)$ *будем обозначать множество* $m \times n$ *матриц* $v^{i,j}(t,w)$*, каждый элемент которых удовлетворяет условию* $v^{i,j} \in \mathfrak{L}^{(n)}$.

Рассмотрим общий вид стохастического дифференциального уравнения. Пусть функции $\sigma \in \mathfrak{L}^{(m\times n)}$, $b \in \mathfrak{L}^{(n)}$. Также будем рассматривать стохастическое дифференциальное (матричное) уравнение

$$X_t = \quad x + \int_s^t b(s, X_s)\,ds + \int_s^t \sigma(s, X_s)\,dB_s, \tag{12}$$

где под интегралом $\int_s^t \sigma^{ij}(s, X_s)\,dB_s^j$ будем понимать t-непрерывную версию одномерного интеграла Ито, которая всегда существует. Последние два интеграла определяют решение $X_t^{s,x}$ дифференциального уравнения (12), начинающееся в s, $\left(X_t^{s,x}\big|_{t=s} = x\right)$.

Потребуем выполнения дополнительных условий. Пусть C, D и $T > 0$ — некоторые константы и отображения $b(*,*) : [0,T] \times R^n \to R^n$, $\sigma(*,*) : [0,T] \times R^n \to R^{n\times m}$ являются измеримыми функциями, удовлетворяющими условиям

$$|b(t,x)| + |\sigma(t,x)| \le \quad C(1+|x|), \quad x \in \quad R^n, \quad t \in \quad [0,T], \tag{13}$$

где $|b|^2 = \sum_{k=1}^n b_k^2$, $|\sigma| = \sum_{i,j=1}^n \sigma_{i,j}^2$, и условию

$$|b(t,x) - b(t,y)| + |\sigma(t,x) - \sigma(t,y)| \le \quad D|x-y|, \quad x, y \in \quad R^n, \quad t \in \quad [0,T]. \tag{14}$$

Выполнение этих условий обеспечивает существование и единственность решения дифференциального уравнения (12).

Заметим, что если функция u_t является константой $(u_t = u)$, то очевидно выполнение условий (13) и (14) для уравнения (11). В уравнении (11)

$$b(t,x) = \quad x(ua + b(1-u)),$$
$$\sigma(t,x) = \quad \alpha u x$$

поэтому

$$|b(t,x)|+|\sigma(t,x)| \le [2ua+b(1-u)](1+|x|)$$
$$|b(t,x)-b(t,y)|+|\sigma(t,x)-\sigma(t,y)| \le [2ua+b(1-u)]|x-y|.$$

Доказано существование и единственность решения дифференциального уравнения (11).

3. Постановка задача оптимального управления

Возвратимся к задаче оптимального управления. Пусть $X_t \in R^n$, B_t — n-мерное броуновское движение, функция управления $u_s \in U \subset R^k$ является $\Im_s$ согласованной и при фиксированном u, функции $b: R \times R^n \times U \to R^n$ и $\sigma: R \times R^n \times U \to R^{n \times m}$. Предположим, что состояние системы в момент времени s описывается стохастическим процессом Ито

$$dX_t = b(t, X_t, u_t)\,dt + \sigma(t, X_t, u_t)\,dB_t. \qquad (15)$$

Относительно этого уравнения будем предполагать, что решение дифференциального уравнения существует и единственно. Пусть $\{X_h^{s,x}\}_{h \ge s}$ — решение уравнения (15) такое, что $X_s^{s,x} = x$, или

$$X_h^{s,x} = x + \int_s^h b(r, X_r^{s,x}, u_r)\,dr + \int_s^h \sigma(r, X_r^{s,x}, u_r)\,dB_r.$$

Обозначим символом $Q^{s,x}$ закон распределения вероятностей для $X_h^{s,x}$:

$$Q^{s,x}\left[w: X_{t_1}(w) \in F_1, X_{t_2}(w) \in F_2, \ldots, X_{t_n}(w) \in F_n\right] =$$
$$= P^0\left[w: X_{t_1}^{s,x}(w) \in F_1, X_{t_2}^{s,x}(w) \in F_2, \ldots, X_{t_n}^{s,x}(w) \in F_n\right],$$

где F_k — борелевские множества и $s \le t_1$. Математическое ожидание относительно этой меры будем обозначать символом $E^{s,x}$.

Пусть $F: R \times R^n \times U \to R$ (функция «нормы полезности») и $K: R \times R^n \to R$ (функция «наследства») — непрерывные функции, G — заданная область в R^2 и T — момент первого после s выхода процесса $\{X_h^{s,x}\}_{h \ge s}$ из множества G.

$$T = T^{s,x}(w) = \inf_{\substack{s<r \\ (r, X_r^{s,x}) \notin G}} r < \infty.$$

Предположим, что $E^{s,x}\left[\int_s^T |F(r, X_r, u_r)|\,dr + |K(T, X_T)|\,\mathfrak{X}_{\{T<\infty\}}\right] < \infty$. Определим функцию качества $J^u(s,x)$ равенством

$$J^u(s,x) = E^{s,x}\left[\int_s^T F(r, X_r, u_r)\,dr + K(T, X_T)\,\mathfrak{X}_{\{T<\infty\}}\right]. \qquad (16)$$

Задача оптимального управления состоит в нахождении для каждого $(s,x) \in G$ такого числа

$$\Phi(s,x) = \inf_{u(t,w)} J^u(s,x) = J^{u^*}(s,x), \qquad (17)$$

где точная верхняя грань берется по всем $\mathfrak{I}_t^{(m)}$ согласованным процессам $\{u_t\}$ со значениями в U. Такое управление u^* называется *оптимальным управлением*, Ф называется *оптимальной функцией качества, или ценой*.

Рассмотрим нашу задачу как задачу оптимального управления. Определим множество $G = \{(r,z); r < t_0, z > 0\}$. Пусть T — момент первого выхода из множества

$$T = T^{s,x}(w) = \inf_{\substack{s<r \\ (r,X_r^{s,x})\notin G}} r = \inf_{\substack{\{s<r\} \\ \{r\ge t_0\}\vee\{X_r^{s,x}\le 0\}}} r < \infty$$

Заметим, что инфинимум ищется для тех r, для которых выполнено хотя бы одно условие: либо $r \ge t_0$, либо $X_r^{s,x} \le 0$. Условие $r \ge t_0$ достаточно очевидно, условие $X_r^{s,x} \le 0$ означает, что нет смысла выбирать $r \ge t_0$, так как прибыль $X_r^{s,x}$ начинает падать.

Итак, задача сводится к нахождению марковского управления $0 < u^* = u^*(t, X_t^{s,x}) < 1$, и значения функции $\tilde{\Phi}(s,x)$, такой чтобы математическое ожидание прибыли $X_t^{s,x}$ было максимальным.

$$\tilde{\Phi}(s,x) = \sup_{\substack{u-\text{марковское управление} \\ 0<u<1}} E^{s,x}\left[X_T^u\right].$$

В этом виде задачу математически решить сложно. Для того чтобы использовать имеющийся математический аппарат, изменим немного задачу. Рассмотрим новое определение.

Определение 5. *Функция* $\varphi:[0,\infty)\to[0,\infty)$ *называется функцией критерия, если она не убывающая, выпуклая, то есть для всех* $x, y > 0$ *и* $0 < \lambda < 1$ *выполнено неравенство* $\varphi(\lambda x + (1-\lambda)y) \le \lambda\varphi(x) + (1-\lambda\varphi(y))$ *и* $\lim\limits_{x\to\infty}\dfrac{\varphi(x)}{x} = \infty$.

Например, функция x^p является функцией критерия при $p > 1$.

Если выбрать функцию критерия N, то исходная задача сводится к нахождению марковского управления $0 < u^* = u^*(t, X_t) < 1$, такого что

$$\Phi(s,x) = \sup_{\substack{u-\text{марковское управление} \\ 0<u<1}} E^{s,x}\left[N\left(X_T^u\right)\right],$$

где T — момент первого выхода из множества $G = \{(r,z); r < t_0, z > 0\}$.

4. Решение задачи оптимального управления

Рассмотрим решение задачи (16) и (17). Все обозначения, рассмотренные в этой задаче, также использованы и ниже.

Для $v \in R$ и $f \in C_0^2(R\times R^n)$ определим оператор

$$\left(L^v f\right)(s,x) = \frac{\partial f}{\partial s} + \sum_{i=1}^n b(s,x,v)\frac{\partial f}{\partial x_i} + \frac{1}{2}\sum_{i,j=1}^n \left(\sigma\sigma^T\right)_{ij}(s,x,v)\frac{\partial^2 f}{\partial x_i \partial x_j}, \tag{18}$$

где $x = (x_1, \ldots, x_n)$.

Рассмотрим утверждение, позволяющее находить управление, которое может быть оптимальным, то есть необходимое условие оптимальности управления.

Напомним одно определение. Точка $y \in \partial G$ называется регулярной для области G относительно процесса X_t, если для τ_G — момента первого выхода процесса X_t из области G справедливо равенство $Q^y(\tau_G = 0) = 1$. Рассмотрим теорему, которая носит название «уравнение Гамильтона-Якоби-Беллмана (HJB)».

Теорема 1. *Определим функцию*

$$\Phi(s,x) = \sup\left\{J^u(s,x), \text{где } u - \text{марковское управление}\right\}.$$

Пусть функция $\Phi \in C^2(G) \bigcap C(\overline{G})$ *удовлетворяет условию*

$$E^{(s,x)}\left[\left|\Phi(X_\alpha)\right| + \int_0^\alpha \left|L^v \Phi(X_t)\right| dt\right] < \infty$$

для всех ограниченных моментов остановки $\alpha < T$, *всех* $(s,x) \in G$, *всех* $v \in U$. *Кроме того, предположим, что* $Q^{s,x}$ *— почти наверное случайная величина* $T < \infty$ *для всех* $(s,x) \in G$ *и что оптимальное марковское управление* u^* *существует. Пусть* ∂G *— регулярная граница области* G *для случайного процесса* $X_t^{u^*}$. *Тогда для всех* $(s,x) \in G$

$$\sup_{v \in R^k}\left\{F(s,x,v) + \left(L^v \Phi\right)(s,x)\right\} = 0$$

и для всех $(s,x) \in \partial G$

$$\Phi(s,x) = K(s,x).$$

Если $u^*(s,x)$ *— оптимальное управление, то выполнено равенство*

$$F\left(s,x,u^*(s,x)\right) + \left(L^{u^*(s,x)}\Phi\right)(s,x) = 0. \qquad (19)$$

Эта теорема с необходимостью устанавливает существование $u^*(s,x)$. То есть, для того чтобы найти u^*, необходимо решить уравнение (19). Рассмотрим достаточное условие. Для этого напомним еще одно определение.

Определение 6. *Пусть* $(\Omega, \Im, P)$ *— вероятностное пространство. Семейство действительных измеримых функций* $\left\{f_j\right\}_{j \in J}$ *на* Ω *называется равномерно-интегрируемым, если*

$$\lim_{M \to \infty}\left(\sup_{j \in J}\left\{\int_{|f_j| > M} \left|f_j\right| dP\right\}\right) = 0.$$

Рассмотрим вопрос о том, как исследовать семейство равномерно-интегрируемых функций.

Теорема 2. *Семейство действительных измеримых функций* $\left\{f_j\right\}_{j \in J}$ *на* Ω *является равномерно-интегрируемым тогда и только тогда, когда существует функция критерия* φ, *такая что справедливо неравенство*

$$\sup_{j\in J}\left\{\int\varphi\left(\left|f_j\right|\right)dP\right\}<\infty. \tag{20}$$

Возвратимся к достаточному условию оптимальности управления.

Теорема 3. *Пусть функция* $\Phi\in C^2(G)\bigcap C\left(\overline{G}\right)$ *удовлетворяет условиям теоремы 1 и условию* $F(s,x,v)+\left(L^v\Phi\right)(s,x)\le 0$ *с граничными условиями*

$$\sup_{t\to T}\Phi(X_t)=K(X_T)\mathfrak{X}_{\{T<\infty\}}\qquad Q^{s,x}-\text{п.н.} \tag{21}$$

такая, что семейство $\left\{\Phi\left(X_\tau\right)\right\}_{\tau<T}$ *равномерно* Q^X *интегрируемо для всех марковских управлений* u *и всех* $(s,x)\in G$.

Тогда для всех марковских управлений u *и всех* $(s,x)\in G$ *имеем* $\Phi(s,x)\ge J^u(s,x)$.

Кроме того, если для каждого $(s,x)\in G$ *определено управление* $u_0=u_0(s,x)$, *при котором*

$$F\left(s,x,u_0(s,x)\right)+\left(L^{u_0(s,x)}\Phi\right)(s,x)=0,$$

то случайная величина u_0 *является оптимальным марковским управлением, или*

$$\Phi(s,x)=J^{u_0}(s,x).$$

Вернемся к нашей задаче. Как сказано в начале работы, $b<a$. Выберем константы α и r из условия

$$0<\frac{a-b}{\alpha^2(1-r)}<1. \tag{22}$$

Дифференциальный оператор L^u, согласно (18), определяется равенством

$$\left(L^uf\right)(t,x)=\frac{\partial f}{\partial t}+x\left(av+b(1-u)\right)\frac{\partial f}{\partial x}+\frac{1}{2}\alpha^2v^2x^2\frac{\partial^2 f}{\partial x^2}. \tag{23}$$

В нашей задаче $F\equiv 0$ и, следовательно, уравнение HJB принимает вид

$$\sup_v\left\{\left(L^u\Phi\right)(t,x)\right\}=0 \tag{24}$$

при $(t,x)\in G$ и

$\Phi(t,x)=N(x)$ для $t=t_0$,

$\Phi(t,0)=N(0)$ для $t<t_0$.

Следовательно, для каждой пары (t,x) требуется найти значение $v=u(t,x)$, которое максимизирует функцию

$$\eta(v)=\left(L^v\Phi\right)=\frac{\partial\Phi}{\partial t}+x\left(b+(a-b)v\right)\frac{\partial\Phi}{\partial x}+\frac{1}{2}\alpha^2v^2x^2\frac{\partial^2\Phi}{\partial x^2}. \tag{25}$$

Для этого найдем производную функции η и приравняем эту производную к нулю.

$$\eta_v^*(v) = \left(L^v\Phi\right) = x(a-b)\frac{\partial\Phi}{\partial x} + \alpha^2 v x^2 \frac{\partial^2\Phi}{\partial x^2} = 0,$$

$$v_0 = u(t,x) = -\frac{(a-b)\frac{\partial\Phi}{\partial x}}{\alpha^2 x\frac{\partial^2\Phi}{\partial x^2}} = -\frac{(a-b)\Phi_x}{\alpha^2 x\Phi_{xx}} \tag{26}$$

Если $\Phi_{xx} = \frac{\partial^2\Phi}{\partial x^2} < 0$, то v_0 — точка максимума. При подстановке этого выражения в (25) и учитывая (24), получим следующую краевую задачу для Ф:

$$\begin{cases} \Phi_t + bx\Phi_x - \frac{(a-b)^2\Phi_x}{2\alpha^2\Phi_{xx}} = 0 & \text{при} \quad t < t_0 \quad \text{и} \quad x > 0 \\ \Phi(t,x) = N(x) & \text{при} \quad t = t_0 \quad \text{или} \quad x = 0. \end{cases}$$

Заметим, что решить эту систему при произвольной функции $N(x)$ очень сложно. Рассмотрим функцию $N(x)$ в виде $N(x) = x^r$, $0 < r < 1$. Решение последней системы, как легко видеть, имеет вид

$$\Phi(t,x) = x^r \exp\left(\left(br + \frac{(a-b)^2 r}{2\alpha^2(1-r)}\right)(t_0 - t)\right) = x^r \exp\left(\lambda(t_0 - t)\right). \tag{27}$$

Подставляя это выражение в (25), имеем

$$L^v(\Phi) = \frac{r\exp\left(\lambda(t_0-t)\right)x^r}{2\alpha^2(1-r)}\left[-\left[(b-a)+\alpha^2(1-r)v\right]^2\right] \le 0.$$

Заметим, что $L^v(\Phi) = 0$ тогда и только тогда, когда $v = u^*(t,x) = \frac{b-a}{\alpha^2(1-r)}$. Согласно неравенству (22) и теореме (3), решение существует.

5. Вывод

Для злоумышленника самой лучшей будет стратегия в каждый момент времени t покупать $\frac{b-a}{\alpha^2(1-r)}X_t$ банковских карт первого вида и, соответственно, $\left(1-\frac{b-a}{\alpha^2(1-r)}\right)X_t$ банковских карт второго вида. Максимальная ожидаемая прибыль от этой стратегии, согласно (27), равна

$$\Phi(t,x) = x^r \exp\left(\left(br + \frac{(a-b)^2 r}{2\alpha^2(1-r)}\right)(t_0 - t)\right).$$

Оценим эту формулу снизу и сверху. Имеем

$$x^r \exp\left(br\left(t_0 - t\right)\right) \le \Phi\left(t, x\right) \le$$
$$\le \quad x^r \exp\left(\left(br + \frac{\left(a-b\right)^2 r}{2\alpha^2\left(1-r\right)}\right)\left(t_0 - t\right)\right) \le$$
$$\le \quad x^r \exp\left(r\left(\frac{a+b}{2}\right)\left(t_0 - t\right)\right)$$

Из последней формулы при данных, взятых из первого раздела, $a = 0.8$ и $b = 0.2$, для $r = 0.5$ и при начальном капитале, равном 1, удвоение капитала произойдет за $2.7 \le t_0 - t \le 3.4$, то есть за три-четыре дня. Напомним, что при покупке карточек первого и второго вида удвоение капитала происходит за 37 и 9 дней соответственно. То есть, очевидно, что применение нашего управления покупкой банковских карт дает очевидную выгоду преступнику.

ЛИТЕРАТУРА

1. Knight F. B. Essentials of Brownian Motion. American Math. Soc., 1981.

2. Оксендаль Б. Стохастические дифференциальные уравнения. — М.: Мир, 2003.

3. Гихман И. И., Скороход А. В. Теория случайных процессов. — М.: Наука, 1975.

4. Розанов Ю. А. Марковские случайные поля. — М.: Наука, 1981.

СВЕДЕНИЯ ОБ АВТОРЕ СТАТЬИ:

Атласов Игорь Викторович. Начальник кафедры автоматизированных информационных систем ОВД. Доктор физико-математических наук, профессор.

Воронежский институт МВД России.

E-mail: vorhmscl@comch.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. 8(473)2623-278.

Atlasov Igor Victorovich. Chief of the chair of automated information systems of the Law Enforcement Agencies. Doctor of physics and mathematics, professor.

Voronezh Instinute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8(473)2623-278.

Ключевые слова к статье: броуновское движение; стохастическое уравнение; интеграл Ито; оптимальное управление.

Key words: Brownian motion; stochastic equation; Ito integral; optimal control.

УДК 519.21

В.С. Дунин,
Дальневосточный юридический институт МВД России

О.И. Бокова,
доктор технических наук, профессор

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ОВД

EVALUATION OF THE EFFICIENCY OF THE SYSTEM OF INTELLECTUAL MANAGEMENT OF SECURITY INFORMATION IN THE INFOCOMMUNICATION SYSTEMS OF THE LAW ENFORCEMENT AGENCIES

Представлена методика оценки эффективности адаптивной интеллектуальной системы защиты информации, модель которой основана на свойствах нечетких и нейронных сетей и имеет иерархическое построение по уровням и механизмам защиты.

The article presents a method of the evaluation of the efficiency of the adaptive intelligent system of information security,whose model is based on the properties of fuzzy and neural networks and has a hierarchical structure of the levels and protection mechanisms.

Для придания необходимых качеств современной системе управления информационной безопасностью в ряде работ [5] предложено создавать интеллектуальные адаптивные системы защиты информации (СЗИ), основывающиеся на свойствах нейронных и нечетких сетей.

Модель адаптивной системы защиты информации в интеллектуальных системах управления характеризуется тем, что это многоуровневая обучаемая иерархическая структура, которая использует экспертные оценки для привнесения априорного опыта в СЗИ в виде системы нечетких продукционных правил. Рассмотрим построение такой структуры на примере разработанной модели (см. рис. 1, 2).

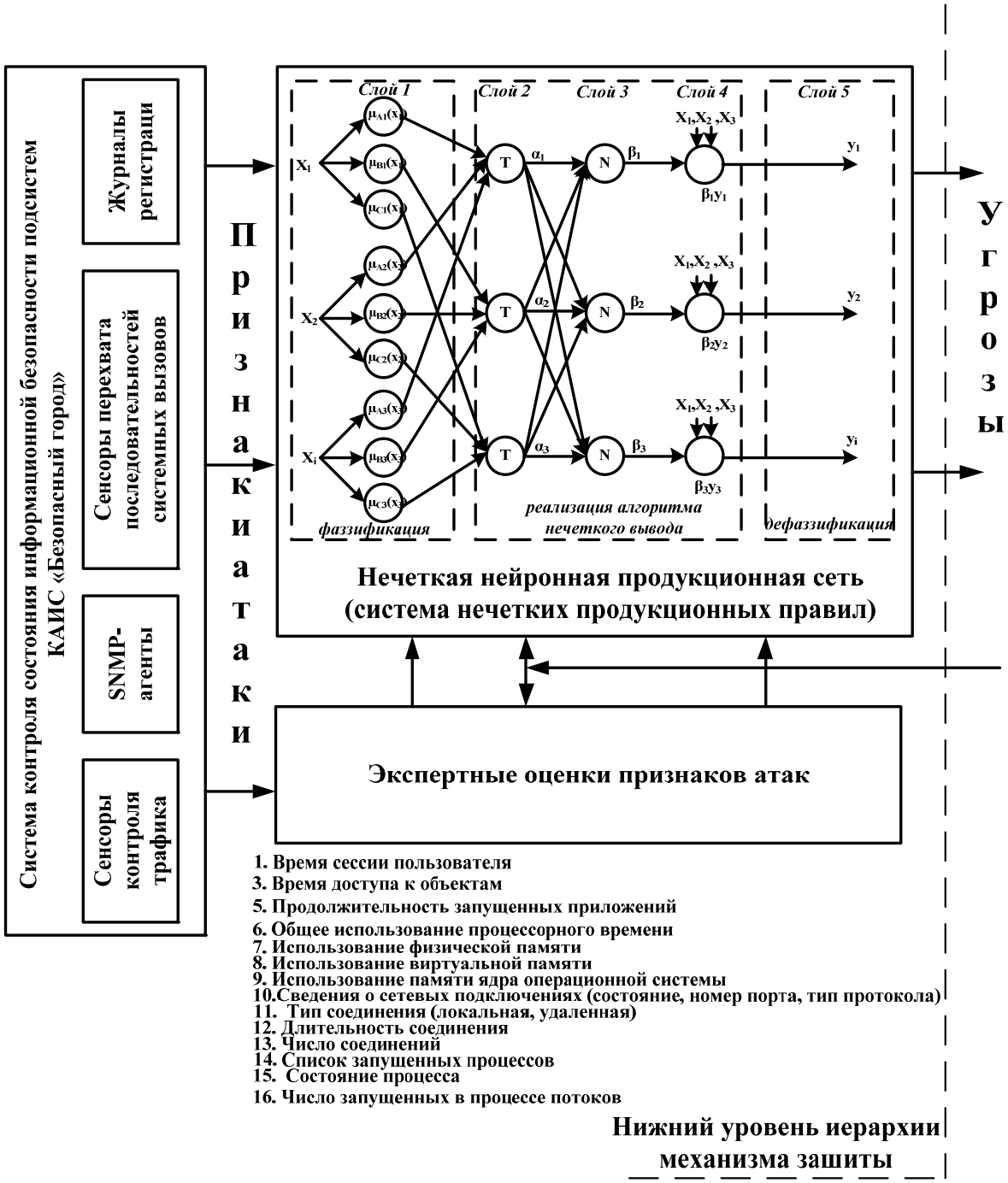


Рис. 1. Модель адаптивной системы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город», нижний уровень иерархии защиты

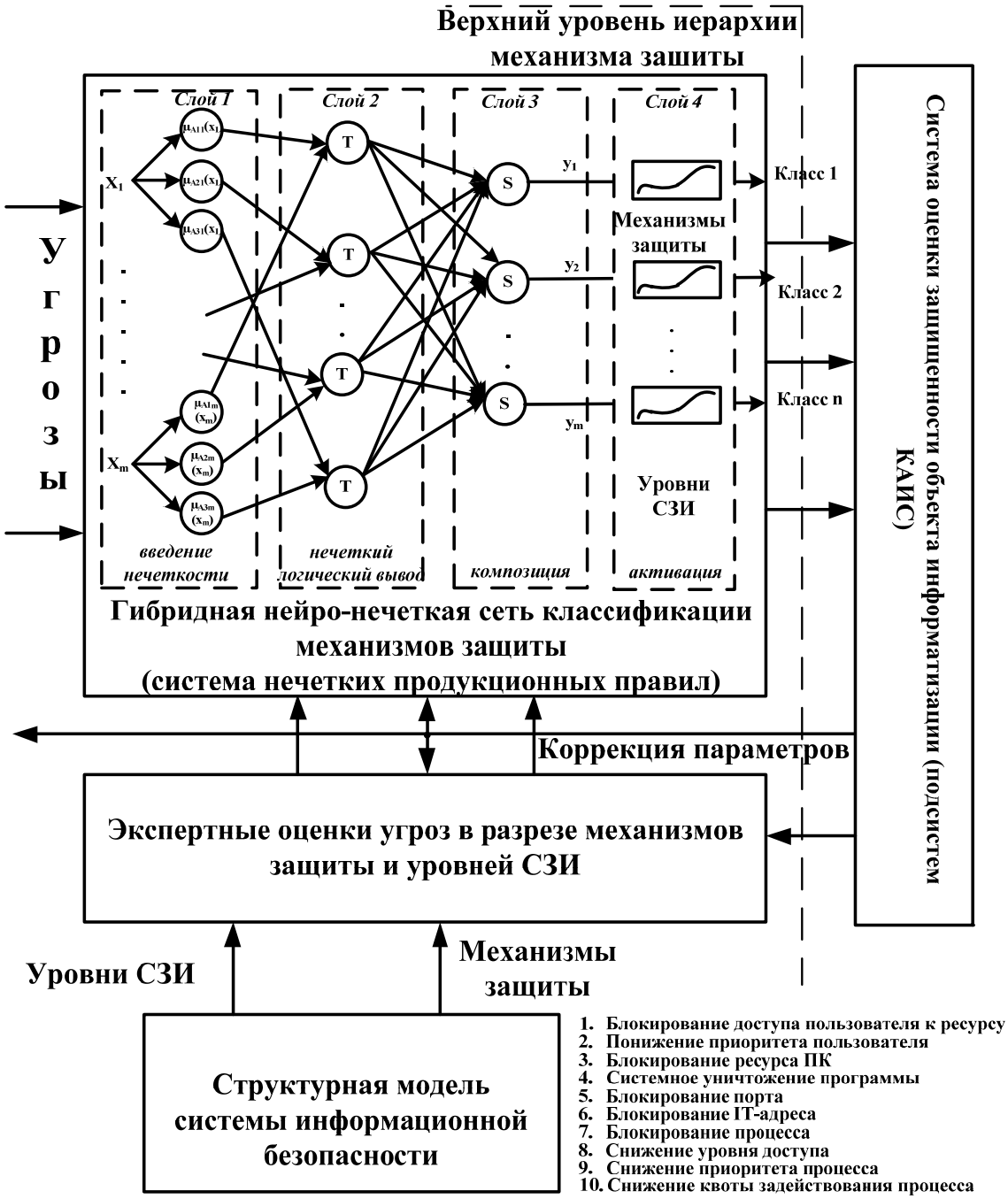


Рис. 2. Модель адаптивной системы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город», верхний уровень иерархии защиты

Данная модель показывает архитектуру построения СЗИ такой инфокоммуникационной системы ОВД, как комплексная автоматизированная интеллектуальная система (КАИС) «Безопасный город», в соответствии с которой определяется структурная модель системы информационной безопасности в виде иерархии уровней механизмов защиты.

Априорный опыт экспертов представляется массивами экспертных оценок, на базе которых формируются системы нечетких продукционных правил для идентификации (классификации) угроз по признакам атак и классификации механизмов защиты на поле угроз.

Необходимость выявлять максимально возможное число атак требует использования в системах защиты подсистем обнаружения аномалий, функционирующих на разных уровнях КАИС [2]. Анализаторы подсистем обнаружения используют исходные данные от сетевых и хостовых сенсоров. На сетевом уровне сетевые датчики (сенсоры) устанавливаются в сегментах сети ЕИТКС ОВД и хостах КАИС. Источниками информации о сетевом трафике являются также встроенные в коммутаторы и маршрутизаторы SNMP-агенты.

Внизу иерархии СЗИ решается задача идентификации (классификации) атак по совокупности признаков, носящих неполный и не вполне достоверный характер. Нечеткая нейронная сеть нижнего уровня СЗИ, исходя из опыта экспертов информационной безопасности, реализует систему нечетких правил типа Такаги-Сугено [1], которая описывает процесс логического вывода получения заключения (тип атаки), используя в качестве нечетких посылок векторы входных признаков (данные от сетевых и хостовых сенсоров).

Предлагаемая нечеткая нейронная продукционная сеть (ANFIS — Adaptive Network-based Fuzzy Inference System) на нижнем уровне может одновременно формировать нечеткие правила и адаптировать функции принадлежности путем модификации весов связей в процессе обучения, и — что самое важное — для этого может применяться классический алгоритм обратного распространения ошибки.

На верхних уровнях иерархии защиты для каждого эшелона многоуровневой СЗИ средства защиты информации используют результаты идентификации (классификации) нижних уровней иерархии в виде посылок системы нечетких продукционных правил для формирования заключений соответствий «угрозы-механизмы защиты». То есть решается задача классификации механизмов защиты (нечеткие заключения) по вектору нечетких признаков угроз, для нейтрализации последствий которых данные механизмы защиты предназначены [4]. Нейронная сеть данного уровня СЗИ представляет собой гибридную нейронную нечеткую сеть (HFNN — Hybrid Fuzzy Neural Networks), являющуюся универсальным аппроксиматором для разных функций принадлежности входных и выходных данных к нечеткому полю множеств [3]. После обучения классическим методом обратного распространения ошибки, схожим с методом обучения сети ANFIS, она будет отражать достоверность нейтрализации заданного в отдельном правиле набора угроз соответствующим механизмом защиты (механизм системного уничтожения программ, механизм блокирования доступа к ресурсу, механизм понижения приоритета пользователя, механизм идентификации и аутентификации и т.д.) определенного эшелона многоуровневой СЗИ.

Верхний уровень иерархии СЗИ также необходим для обобщения результатов (посылок) в виде активности механизмов защиты, частоты реализации и ущерба от угрозы с целью формирования системы нечетких продукционных правил — заключений о целесообразности расширения состава активированных механизмов защиты по отдельным эшелонам СЗИ [4]. Активация механизмов защиты производится, если интегральные оценки, учитывающие величину потенциального ущерба, частоту реализации угроз и достоверность нейтрализации угроз данным механизмом защиты, превышают заданные пороговые значения.

Многоуровневая модель информационной безопасности данной системы на первом этапе соответствует минимальной активации потенциальных механизмов защиты и полноте информационного поля известных угроз.

На втором этапе модель динамически пополняется путем перевода механизмов защиты из статуса «потенциальный» в статус «активированный» и привязки активированного механизма к соответствующему эшелону модели СЗИ. Увеличивается число элементов в подмножестве заданных угроз, как за счет включения элементов из множества известных угроз, так и за счет пополнения самого множества известных угроз ранее неизвестными угрозами. Далее возможно расширение множества потенциальных механизмов защиты за счет описания в виде нечетких продукционных правил и последующей реализации ранее отсутствующих механизмов защиты.

При последующей адаптации произойдет обучение СЗИ под отсутствующий механизм защиты информации, направленный на нейтрализацию неспецифицированной угрозы. Анализ дополнительного нечеткого продукционного правила позволяет сформировать спецификацию на проектирование отсутствующего в системе средства или механизма защиты информации.

Задавая пороговые значения для величины нечеткого заключения продукционных правил, определяющего степень использования *i*-го механизма защиты в формировании значения итоговой защищенности системы, можно определять как наименее задействованные, так и эффективно используемые механизмы в обеспечении безопасности защищаемой системы.

Решение о расширении классификаций атак и механизмов защиты производится в соответствии с системой оценок достоверности нейтрализации угроз в разрезе отдельных механизмов защиты или отдельных эшелонов СЗИ и аналогичных оценок потенциального ущерба, также соотносимых с отдельными механизмами защиты или отдельными эшелонами СЗИ [9].

Если рассматривать информационно-телекоммуникационные подсистемы КАИС «Безопасный город», являющиеся сегментами инфокоммуникационной интеграции ЕИТКС ОВД, как совокупность рабочих станций, серверов, межсетевых шлюзов, маршрутизаторов, аппаратуры и каналов связи, то при создании СЗИ следует использовать ключевые принципы ее построения, которые обобщают основные положения современной концепции ЗИ:

комплексность и *согласованность* использования широкого спектра методов и средств защиты при построении целостной системы защиты, не содержащей слабых мест на стыках ее компонентов;

дифференциацию мер защиты в зависимости от критичности (важности) информации и потенциально возможных угроз информационным ресурсам;

разумную достаточность механизмов защиты, что означает правильность выбора достаточного уровня защиты, при котором затраты на СЗИ и размер возможного ущерба (риск) были бы приемлемыми.

На основе анализа всех возможных каналов несанкционированного доступа к информационной среде КАИС «Безопасный город» и в соответствии с основными принципами построения системы защиты предлагается трехрубежная модель СЗИ [3] (см. рис. 3).

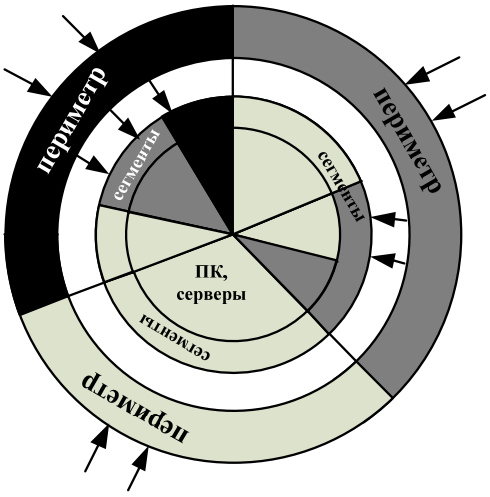


Рис. 3. Трехрубежная модель СЗИ

Первый рубеж — это периметр объекта защиты, набор функциональных подсистем, включающих средства и механизмы системной защиты от внешних угроз злоумышленника и потенциально возможных деструктивных воздействий удаленного пользователя.

Второй рубеж — набор функциональных подсистем защиты сетевого сегмента от потенциально возможных межсегментных и удаленных атак.

Третий рубеж включает в себя набор функциональных подсистем, обеспечивающих защиту информационной среды отдельного персонального компьютера, сервера.

В некоторых работах отмечается, что гибридные атаки, использующие множество стратегий нападения, могут быть остановлены только многоуровневой, эшелонированной линией обороны (см. рис. 4).

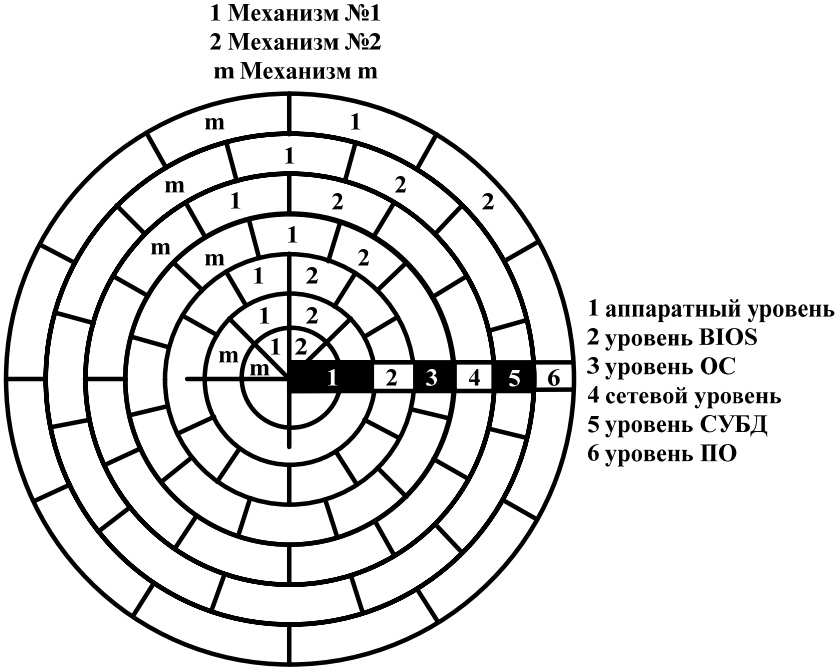


Рис. 4. Распределение механизмов защиты по эшелонам СЗИ

Таким образом, модель СЗИ включает в себя три компонента: модель защиты периметра объекта защиты, модель защиты сетевого сегмента, модель защиты ПК и сервера. Модель каждого рубежа защиты является N-уровневой и включает в себя N морфологических матриц в зависимости от уровня критичности (важности) обрабатываемой на объекте защиты информации.

Предложим метод оценки эффективности системы интеллектуального управления защитой информации, учитывающий действительную загруженность механизмов защиты по нейтрализации последствий атак, возможность адаптации СЗИ к изменению поля угроз и изменение структуры многоуровневой СЗИ [5].

Стоит отметить, что под оценкой эффективности подразумевается процедура, направленная на определение качественных и количественных показателей эффективности, выявление критических элементов, а также нахождение интегрального показателя эффективности системы в целом, который характеризовал бы степень достижения целей, поставленных при её создании. При этом сам показатель эффективности — это величина, характеризующая степень достижения системой стоящей перед ней цели. Значение показателей, при которых система удовлетворяет предъявляемым к ней требованиям, в свою очередь, именуется критерием эффективности.

В работе [8] предложено в качестве оценки защищенности использовать рейтинговый показатель, который учитывает распределение механизмов защиты по эшелонам многоуровневой модели системы информационной безопасности и изменение вероятности достижения злоумышленником объекта защиты в зависимости от эшелона многоуровневой модели СЗИ. К недостаткам модели следует отнести статичный характер оценки защищенности информационной системы, не учитывающей такие параметры, как ущерб от реализации угроз информационной безопасности и частота осуществления атак.

В работе [9] защищенность оценивается исходя из ущерба от реализации в системе ИТ угроз, носящих случайный характер, который оценивается через коэффициенты опасности угроз. Причем коэффициенты опасности представляются нечеткими величинами, а показатель защищенности системы ИТ определяется посредством формируемой методом экспертных оценок матрицы нечетких отношений между коэффициентом опасности совокупности угроз и степенью защищенности системы ИТ. Недостатком подобного оценивания является отсутствие привязки показателей защищенности к местоположению МЗ в структуре СЗИ. Как и в предыдущем случае, сохраняется статичность оценки защищенности ИБ системы ИТ.

Известные [7—9] оценки отражают лишь статическое состояние объекта защиты, исходя из наличествующих механизмов защиты, не учитывают действительную загруженность механизмов защиты по нейтрализации последствия атак, динамику изменения поля угроз, возможность адаптации СЗИ к изменению поля угроз, не дают указаний на изменение состава механизмов защиты и структуры многоуровневой СЗИ.

Проведенный анализ показал необходимость разработки обобщенного количественного показателя для оценки свойства «защищенность» информационной системы и «эффективность» для оценки системы защиты информации, которые должны объединить положительные стороны известных подходов с целью его дальнейшего использования в качестве целевой функции для оптимизации структуры информационной системы по критерию «стоимость/защищенность»[6].

Покажем комплексный подход для оценки событий информационной безопасности, показателей защищенности и эффективности рассматриваемой интеллектуальной системы защиты информации [6].

Первый шаг. Исходные данные (экспертные оценки) представляются в матричной форме, учитывая показания агентов и сенсоров информационного контроля состояния информационной безопасности. Для каждого эшелона многоуровневой СЗИ (см. рис. 3) оценивается достоверность нейтрализации угроз механизмами защиты с последующим формированием матрицы достоверности «механизмы защиты-угрозы» *MT:*

$$MT_{mxp} = \left| \begin{array}{ccc} mt_{11} & mt_{12} & mt_{1p} \\ mt_{21} & mt_{22} & mt_{2p} \\ \hline mt_{m1} & mt_{m2} & mt_{mp} \end{array} \right|, \qquad (1)$$

где $i = 1\ldots..m$ — число механизмов защиты; $j = 1\ldots..p$ — число известных угроз, и матрицы достоверности «угрозы-эшелоны» *TE:*

$$TE_{pxn} = \left| \begin{array}{ccc} te_{11} & te_{12} & te_{1n} \\ te_{21} & te_{22} & te_{2n} \\ \hline te_{p1} & te_{p2} & te_{pn} \end{array} \right|, \qquad (2)$$

где $i = 1\ldots.. p$ — число известных угроз; $j = 1\ldots.. n$ — число эшелонов СЗИ.

Для каждого эшелона многоуровневой СЗИ оценивается уровень потенциального ущерба и формируются матрицы «эшелоны-ущерб» *ET:*

$$ET_{nxp} = \left| \begin{array}{ccc} et_{11} & et_{12} & et_{1p} \\ et_{21} & et_{22} & et_{2p} \\ \hline et_{n1} & et_{n2} & et_{np} \end{array} \right|, \qquad (3)$$

где $i = 1\ldots.. n$ — число эшелонов СЗИ; $j = 1\ldots... p$ — число известных угроз, и матрицы «ущерб-механизм защиты» *TM:*

$$TM_{pxm} = \left| \begin{array}{ccc} tm_{11} & tm_{12} & tm_{1m} \\ tm_{21} & tm_{22} & tm_{2m} \\ \hline tm_{p1} & tm_{p2} & tm_{pm} \end{array} \right|, \qquad (4)$$

где $i = 1\ldots.. p$ — число известных угроз; $j = 1\ldots. m$ — число механизмов защиты.

Второй шаг. Для каждого эшелона многоуровневой СЗИ экспертные оценки в виде системы нечетких продукционных правил отображаются в структуре нейро-нечетких сетей. В процессе последующей адаптации нечетких НС на обучающей выборке, соответствующей некоторому подмножеству поля известных угроз, производится автоматическая коррекция системы нечетких продукционных правил, а также показателей потенциального ущерба и достоверности (истинности) нейтрализации набора угроз соответствующим эшелоном или МЗ многоуровневой СЗИ. Корректность исходных экспертных оценок может быть проверена сопоставлением интегральных оценок защищенности до и после процесса обучения нейро-нечетких СЗИ [7].

Третий шаг. Интегральные оценки защищенности получают в результате операций над матрицами. В частности, умножение матриц достоверности «МЗ-угрозы» MT и «угрозы-эшелоны» TE позволяет получить матрицу «МЗ-эшелоны» ME — матрицу

достоверности активации известных механизмов защиты, распределенных по эшелонам многоуровневой СЗИ, для нейтрализации известных угроз:

$$ME_{mxn} = \begin{vmatrix} me_{11} & me_{12} & me_{1n} \\ me_{21} & me_{22} & me_{2n} \\ me_{m1} & me_{m2} & me_{mn} \end{vmatrix}, \quad (5)$$

где $i = 1.....\ m$ — число механизмов защиты; $j = 1....\ n$ — число эшелонов СЗИ, а умножение матриц потенциального ущерба «эшелоны-ущерб» *ET* и «ущерб-МЗ» *TM*-матрицу потенциального ущерба «эшелоны-МЗ» *EM,* отражающую распределение потенциального ущерба от реализации известных угроз по механизмам защиты и эшелонами многоуровневой СЗИ

$$EM_{nxm} = \begin{vmatrix} em_{11} & em_{12} & em_{1m} \\ em_{21} & em_{22} & em_{2m} \\ em_{n1} & em_{n2} & em_{nm} \end{vmatrix}, \quad (6)$$

где $i = 1.....\ n$— число эшелонов СЗИ, $j = 1.....m$— число механизмов защиты.

Получаемые при этом промежуточные оценки в виде строки

$$x_j = \sqrt[m]{\prod_{j=1}^{m} me_{ij}}, j = 1.....n, \quad (7)$$

и столбца

$$\mathrm{x_i} = \sqrt[\mathrm{n}]{\prod_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{me_{ij}}}, \mathrm{i} = 1.....\mathrm{m} \quad (8)$$

интегральных показателей характеризуют активность использования отдельного механизма защиты либо отдельного эшелона в рамках многоуровневой СЗИ, а также позволяют оценить потенциальный ущерб в разрезе механизмов защиты и эшелонов системы информационной безопасности.

Сопоставление интегральных показателей в пределах строки позволяет выявить наиболее задействованные эшелоны в многоуровневой модели СЗИ по нейтрализации поля действующих на систему угроз, а сопоставление интегральных показателей в пределах столбца позволяет выявить наиболее задействованные механизмы защиты в многоуровневой СЗИ.

Анализ интегральных показателей матрицы достоверности «угрозы-механизмы защиты» дает возможность обосновать целесообразность использования механизма защиты в составе соответствующего эшелона многоуровневой СЗИ.

Четвертый шаг. Дальнейшие операции над матрицами *ME* и *EM* дают возможность обобщить в диагональных элементах итоговой матрицы как показатель достоверности активации механизма защиты в результате атаки, так и потенциальный ущерб от ее реализации.

Умножением матрицы достоверности *ME* и матрицы потенциального ущерба *EM* получают квадратную матрицу достоверности потенциального ущерба «механизм защиты-механизм защиты» *MM:*

$$MM_{mxm} = \begin{vmatrix} mm_{11} & mm_{12} & mm_{1m} \\ mm_{21} & mm_{22} & mm_{2m} \\ mm_{m1} & mm_{m2} & mm_{mm} \end{vmatrix}, \quad (9)$$

где $i = j = 1... m$ — число МЗ, а умножением матрицы *EM* и матрицы *ME* получают квадратную матрицу достоверности потенциального ущерба «эшелоны-эшелоны» *EE:*

$$EE_{nxn} = \begin{vmatrix} ee_{11} & ee_{12} & ee_{1n} \\ ee_{21} & ee_{22} & ee_{2n} \\ ee_{n1} & ee_{n2} & ee_{nn} \end{vmatrix}, \quad (10)$$

где $i = j = 1,..., n$ — число эшелонов СЗИ.

Для матрицы *MM* в качестве обобщающего показателя можно рассматривать вектор, образованный диагональными элементами $mm_{ij} = p_i$, $i = j = 1…m$, матрицы – вектор достоверности распределения потенциального ущерба по механизмам защиты СЗИ

$$P_{1xm} = (p_1, p_2, ... p_m), \quad (11)$$

а для матрицы *EE* — вектор из ее диагональных элементов $ee_{ij} = d_i$, $i = j = 1….n$, вектор достоверности распределения ущерба по эшелонам СЗИ

$$D_{1xn} = (d_1, d_2, ...d_n). \quad (12)$$

Пятый шаг. В качестве интегральных оценок защищенности инфокоммуникационной системы КАИС «Безопасный город» в разрезе механизмов защиты можно использовать рейтинговый показатель R_M длину *m*-мерного вектора P_{1xm}

$$R_M = |P_{1xm}| = \sqrt{\sum_{i=1}^{m} p_i^2}, \; i = 1.....m, \quad (13)$$

а в разрезе эшелонов СЗИ — рейтинговый показатель R_E — длину *n*-мерного вектора D_{1xn}

$$R_E = |D_{1xn}| = \sqrt{\sum_{i=1}^{n} d_i^2}, \; i = 1.....n. \quad (14)$$

Текущую эффективность интеллектуальной СЗИ целесообразно оценить в относительных величинах, используя в качестве пороговых значений максимальные значения рейтинговых показателей R_{Mmax} и R_{Emax}, учитывающие достоверную активацию во всех эшелонах многоуровневой СЗИ только активированных механизмов защиты, предотвращающих по каждому из механизмов защиты нанесение ущерба, равного максимально допустимому.

$$з_M = \frac{R_M}{R_{M\,max}}, \quad (15)$$

$$з_E = \frac{R_E}{R_{E\,max}}. \quad (16)$$

Показатели применимы для оценки защищенности систем по множеству известных угроз и по подмножеству угроз: нарушения целостности, конфиденциальности, доступности информации.

С ростом сложности объектов информатизации, изменением множества и характера угроз информационной безопасности, особенно угроз несанкционированного удаленного доступа к ресурсам и процессам критических информационных систем, задача количественной оценки защищенности является актуальной.

Корректная оценка защищенности критических информационных систем необходима для выполнения сравнения аналогичных по назначению и уровню сложности систем либо для мониторинга динамики уровня защищенности конкретной информационной системы во времени.

ЛИТЕРАТУРА

1. Дунин В.С., Бокова О.И., Хохлов Н.С. Построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД на основе нечеткой нейронной продукционной сети // Вестник Воронежского института МВД России. — 2011. — №2. — С. 48 — 59.

2. Дунин В.С. К вопросу о построении модели управления подсистемы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город» // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. материалов Всероссийской научно-практической конференции курсантов, слушателей, студентов, адъюнктов и молодых специалистов. — Воронеж: Воронежский институт МВД России, 2011. — С. 91—92.

3. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. — М.: Горячая линия — Телеком, 2007. — 284 с., ил.

4. Нестерук Г.Ф., Куприянов М.С., Елизаров С.И. К решению задачи нейронечеткой классификации // Сб. докл. VI меж.конф. SCM-2003. — СПб.: СПГЭТУ, 2003. — Т. 1. — С. 244—246.

5. Адаптивные средства обеспечения безопасности информационных систем / Нестерук Ф.Г. [и др.]. — СПб.: Изд-во Санкт-Петербургского политехнического университета, 2008.

6. Суханов А.В. Оценки защищенности информационных систем // Журнал научных публикаций аспирантов и докторантов. — 2008. — №4.

7. Повышение избыточности информационных полей адаптивных классификаторов системы информационной безопасности / Нестерук Г.Ф. [и др.] // Специальная техника. — 2006. — №1.

8. Теоретические основы компьютерной безопасности / Девянин П.Н. [и др.]. — М.: Радио и Связь, 2000.

9. Осовецкий Л., Шевченко В. Оценка защищенности сетей и систем // Экспресс-электроника. — 2002. — №2—3. —С.20—24.

СВЕДЕНИЯ ОБ АВТОРАХ СТАТЬИ:

Дунин Вадим Сергеевич. Преподаватель кафедры информационного и технического обеспечения ОВД. Адъюнкт заочной формы обучения кафедры инфокоммуникационных систем и технологий Воронежского института МВД России.

Дальневосточный юридический институт МВД России.

E-mail: dvs_82@mail.ru

Россия, 680052, Хабаровск, переулок Казарменный, 15. Тел. 8(4212) 29-47-86.

Бокова Оксана Игоревна. Начальник кафедры инфокоммуникационных систем и технологий. Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: OBokova@pochta.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. 8(473) 262-33-85.

Dunin Vadim Sergeevich. The lecturer of the chair of Information and Technical Maintenance of the Law Enforcement Agencies.The post-graduate cadet of correspondence form education of the chair of Infocommunication Systems and Technologies of Voronezh Institute of the Ministry of the Interior of Russia.

Far East Law Institute of the Ministry of the Interior of Russia.

Work address: Russia, 680052, Khabarovsk, Kazarmenny lane, 15. Tel. 8(4212) 29-47-86.

Bokova Oksana Igorevna. The chief of the chair of Infocommunication Systems and Technologies. Doctor of technical sciences, professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8(473) 262-33-85.

Ключевые слова к статье: нечеткая нейронная продукционная сеть; нейро-нечеткая классификация; адаптивная системазащиты информации; инфокоммуникационная система; оценка эффективности, показатель защищенности.

Key words: rule-based fuzzy neural network; neuro-fuzzy classification; adaptive system of information protection; infocommunication system; evaluation of the efficiency; measure of protection.

УДК 621.391

В.С. Дунин,
Дальневосточный юридический институт МВД России

Н.С. Хохлов,
доктор технических наук, профессор

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЛЕКСНОЙ АВТОМАТИЗИРОВАННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ «БЕЗОПАСНЫЙ ГОРОД»

THE MODEL OF INFORMATION SECURITY THREATS OF THE INTEGRATED AUTOMATED INTELLECTUAL SYSTEM “SAFE CITY”

Рассматривается модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город» с позиции теории множеств, учитывая внутрисегментные и межсегментные вторжения злоумышленников.

The article deals with description of the model of information security threats of integrated automated intellectual system «Safe city» from the position of set theory, given the inside-and inter-segment intrusion of attackers.

Комплексная автоматизированная интеллектуальная система (КАИС) «Безопасный город» представляет собой территориально-распределенную систему безопасности, состоящую из множества необходимых подсистем функционирования, объединенных единой транспортной средой — интегрированной мультисервисной транспортной средой (ИМТС) ОВД [1]. Некоторые подсистемы отличаются своей внутренней инфраструктурой, наличием собственных СУБД, интеллектуальными средствами поддержки и распознавания образов. Многие из них являются самостоятельными информационными системами, автоматизирующими процессы обработки, хранения и передачи данных как через открытые информационные сегменты единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, так и через сегменты ограниченного распространения (конфиденциальный и секретный контур), доступ к которым осуществляется посредством удаленного подключения субъектов (пользователи или процессы подсистем КАИС) к выделенным им информационным ресурсам.

Разнородность программно-аппаратного обеспечения подсистем КАИС, огромное количество неоднозначно классифицируемых данных (признаков атак), получаемых от сетевых и хостовых сенсоров, сложность оценки событий информационной безопасности, возможные реализации угроз безопасности информации через обнаруживаемые злоумышленником уязвимости указывают на необходимость создания требуемой системы защиты информации.

Описание угроз безопасности, построение их модели позволяет адекватно оценить уровень опасности и предложить необходимую архитектуру подсистемы защиты информации КАИС «Безопасный город» [2]. В данной статье для построения такой модели проведем анализ угроз, направленных на информационные ресурсы подсистем КАИС, учитывая данные, получаемые сенсорами маршрутизаторов, коммутаторов, межсетевых экранов (МСЭ), систем обнаружения аномалий (СОА) и вторжений (СОВ).

В настоящее время подавляющее число угроз информационной безопасности принципиально могут быть реализованы только в процессе функционирования информационных систем [3], при этом логическое вторжение является наиболее результативным для злоумышленника. Логическое вторжение обычно делится на внутрисистемное и удаленное. При внутрисистемном вторжении предполагается, что нарушитель уже имеет учетную запись в системе как пользователь с невысокими привилегиями и совершает атаку на систему для получения дополнительных привилегий. Удаленное вторжение заключается в попытке проникновения в систему с удаленной машины (хоста) участников информационного обмена сети ЕИТКС ОВД. Это атаки, выполняемые при постоянном участии человека, и атаки, выполняемые специальными программами: атаки на информацию, хранящуюся на внешних запоминающих устройствах, атаки на информацию, передаваемую по линиям связи, атаки на информацию, обрабатываемую в памяти компьютера [4].

Основная цель практически любой атаки при реализации угрозы — получение несанкционированного доступа к информации.

Для описания угрозы, представляющей собой канал несанкционированного доступа (реализация сетевой атаки, деструктивные воздействия вредоносных программ, инсайдерские атаки), необходимо указать субъект доступа, путь распространения угрозы и информационный объект, к которому осуществляется несанкционированный доступ, нарушающий правила разграничения. Такая угроза может быть описана кортежем [4]:

$$U = \langle S, К, Б_с, Б_х, П, ИО(С) \rangle, \quad (1)$$

где S — источник угрозы, т.е. субъект доступа (пользователь (инсайдер), внешний злоумышленник или запущенные ими процессы); $К$ — оборудование в канале связи (коммутаторы, маршрутизаторы и др.); $Б_с$, $Б_х$ — сервисы безопасности на пути распространения угрозы, соответственно, сетевые и хостовые (МСЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и др.); $П$ — протоколы и пакеты; $ИО$ — информационный объект доступа (в конкретном сетевом сегменте ограничения $С$).

В соответствии с рекомендуемыми в [5] основными принципами построения архитектуры безопасности сети зададим три категории ограничения информации: открытая, конфиденциальная и секретная. Тогда множество информационных объектов $ИО$ (информационные ресурсы конфиденциального, секретного и открытого контуров) в сети ЕИТКС представляет собой объединение множеств:

$$ИО = ИО^о \cup ИО^к \cup ИО^с, \quad (2)$$

где $ИО^{о}$ — множество информационных объектов категории «открыто»; $ИО^{к}$ — множество информационных объектов категории «конфиденциально»; $ИО^{с}$ — множество информационных объектов категории «секретно».

Множество сегментов сети C также представляет собой объединение множеств:

$$C = C^{o} \cup C^{к} \cup C^{c}, \quad (3)$$

где $C^{o}, C^{к}, C^{c}$ — подмножества сегментов, в которых хранится и обрабатывается информация, соответственно, с открытым, конфиденциальным и секретным уровнем ограничения;

$$C^{o} = \left\{ c_k^{o}, k \in [1, K] \right\}, \quad (4)$$

где K — число сегментов, в которых хранится и обрабатывается информация категории «открыто»;

$$C^{к} = \left\{ c_l^{к}, l \in [1, L] \right\}, \quad (5)$$

где L — число сегментов, в которых хранится и обрабатывается информация категории «конфиденциально»;

$$C^{c} = \left\{ c_m^{c}, m \in [1, M] \right\}, \quad (6)$$

где M — число сегментов, в которых хранится и обрабатывается информация категории «секретно».

На хостах хранится и обрабатывается информация с определенным для сегмента уровнем ограничения. Зададим множество хостов в каждом сегменте через характеристические предикаты [6]:

$$\mathrm{X}_{\mathrm{k}}^{\mathrm{o}} = \left\{ \mathrm{x}_{\mathrm{k_i}}^{\mathrm{o}} : \mathrm{x}_{\mathrm{k_i}}^{\mathrm{o}} \text{ - узел в сегменте } \mathrm{C}_{\mathrm{k}}^{\mathrm{o}} \right\}, \mathrm{i} \in [1, \mathrm{I_k}]; \quad (7)$$

$$X_l^k = \left\{ x_{l_j}^k : x_{l_j}^k \text{ - узел в сегменте } C_l^k \right\}, j \in [1, J_l]; \quad (8)$$

$$X_m^c = \left\{ x_{m_k}^c : x_{m_k}^c \text{ - узел в сегменте } C_m^c \right\}, k \in [1, K_m]. \quad (9)$$

Множество субъектов доступа, внешних или внутренних, можно рассматривать как источники угроз, под которыми понимается атакующая программа или пользователь, непосредственно осуществляющий воздействие на сетевой сегмент информационной инфраструктуры КАИС «Безопасный город».

По расположению субъекта доступа относительно атакуемого объекта угрозы подразделяются на внешние и внутренние (внутрисегментные и межсегментные) [4].

Внешние угрозы — это потенциально возможные действия, заключающиеся в поиске и использовании той или иной уязвимости, предпринимаемые: злоумышленником в целях проникновения с удаленного хоста в защищаемую систему, получения прав на удаленный доступ к ресурсам подсистем КАИС и хищения данных; удаленным пользователем, имеющим легальные права, пытающимся превысить уровень своих полномочий.

Внутренние угрозы связаны с нарушением принятой политики безопасности: нелегальным поведением пользователя на хосте (ПК или сервере), попытками доступа пользователя к информационным ресурсам, уровень ограничения которых превышает его уровень доступа (попытки сетевых соединений, запуска приложений, реализации запросов к СУБД).

Множество угроз включает в себя подмножества внешних и внутренних угроз:

$$U = U^{вн} u U^{внш}. \quad (10)$$

В свою очередь, подмножество внутренних угроз включает в себя подмножества $U_{m(l)}{}^{вн}$ и $U_{ml(k)}{}^{вн}$, где

$$U_{m(l)}{}^{вн} = \left\langle S^k, К, Б_с, Б_х, П, ИО^c \left(C^c \right) \right\rangle . \quad (11)$$

Здесь $U_{m(l)}^{вн}$ — угроза информационным объектам категории ограничения «секретно» ($ИО^c$) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем ограничения «конфиденциально» (S^k), обрабатываемой в сегментах с ограничением «конфиденциально» или «открыто» и пытается превысить свои привилегии;

$$U_{ml(k)}^{вн} = \left\langle S^o, К, Б_c, Б_x, П, ИО^k\left(C^k\right) \cup ИО^c\left(C^c\right)\right\rangle — \quad (12)$$

угроза информационным объектам категории ограничения «секретно» ($ИО^c$) и «конфиденциально» ($ИО^k$) в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к «открытой» информации (S^o), обрабатываемой в сегментах сети с «открытым» доступом и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем

$$U^{внш} = \left\langle S^{внш}, К, Б_c, Б_x, П, ИО(C)\right\rangle. \quad (13)$$

Таким образом, получено описание угроз безопасности исследуемого объекта, при этом источниками внутренних угроз являются субъекты и процессы, описываемые множествами S^k, S^o, источниками внешних угроз — субъекты и процессы, описываемые множеством $S^{внш}$.

Множество внешних субъектов доступа — это объединение множеств

$$S^{внш} = S_r^{п.внш} \cup S_r^{внш}, r \in [1, R], \quad (14)$$

где $S_r^{п.внш}$ — внешние пользователи, обладающие правами доступа (авторизованные удаленные участники информационного обмена); $S_r^{внш}$ — внешние пользователи, обладающие возможностью несанкционированного доступа (неавторизованные участники информационного обмена других сегментов ЕИТКС ОВД); R — число точек доступа через периметр сети КАИС (совокупность инфокоммуникационного оборудования, заключенная в единое кольцо информационного обмена локальной сети и имеющая доступ во внешние сети — к другим контурам ЕИТКС ОВД).

Введем множество функциональных индикаторов *И* — значений контролируемых параметров, с помощью которых фиксируются отдельные события информационной безопасности. Функциональные индикаторы отражают результаты контроля: изменений правил МСЭ; соответствия настроек других сервисов безопасности политике безопасности; изменений привилегий пользователей; системных вызовов; попыток доступа; состояния соединений.

Поскольку одним из эффективных способов идентифицировать угрозу (атаку) является анализ комбинаций поведений, предлагается сопоставить множеству возможных путей распространения атаки множество индикаторов. Тогда признак того, что подозрительная активность является угрозой, может быть оценен числом индикаторов на пути распространения атаки. Для идентификации внутренних атак предлагается использовать два типа индикаторов: системные и сетевые (хостовые), для идентификации внешних вторжений дополнительно использовать индикаторы, отображающие аномальные события на периметре сети КАИС.

Зададим множество путей распространения атак с помощью характеристического предиката [6]:

$$\mathrm{P} = \{\mathrm{p_i} : \mathrm{p_i} \text{ - путь распространения атаки }\}, \mathrm{i} \in \left[1, \mathrm{I_p}\right]; \quad (15)$$

$$I_p = Q^o + Q^к + Q^c, \quad (16)$$

где $Q^o, Q^к, Q^c$ — число путей распространения атак к узлам в сегментах, в которых хранится и обрабатывается информация с уровнем ограничения, соответственно «открытая», «конфиденциальная», «секретная».

Множество индикаторов является объединением подмножеств:

$$И = И_o^к \cup И_o^c \cup И_к^c \cup И_{пер}, \quad (17)$$

где $И_o^к$ — подмножество индикаторов, фиксирующих попытки доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «конфиденциально»; $И_o^c$ — подмножество индикаторов, фиксирующих попытку доступа субъекта с «открытым» уровнем доступа к объекту с уровнем ограничения «секретно»; $И_{пер}$ — подмножество индикаторов, фиксирующих попытки проникновения на периметре.

Заданное множество индикаторов и путей распространения атак позволяет внести дополнительные экспертные знания о количестве событий информационной безопасности в систему построения нечетких продукционных правил [7].

Предложенное описание модели угроз показывает основные элементы канала несанкционированного доступа (субъект доступа, путь распространения атаки и информационный объект) к информации, циркулирующей на разных уровнях сетевого инфокоммуникационного взаимодействия (контуры безопасности, хосты сегмента, периметр сети) КАИС и ЕИТКС ОВД, учитывающего показания индикаторов событий информационной безопасности от маршрутизаторов, межсетевых экранов, систем обнаружения аномалий и вторжений. Обозначается подход для создания модели системы защиты информации КАИС «Безопасный город».

Таким образом, приведено формализованное построение угроз безопасности КАИС «Безопасный город» с позиции теории множеств с учетом сложности, неоднозначности (нечеткости), неопределенности оценки событий информационной безопасности в условиях информационного противоборства. Такое описание является математической основой построения моделей трудно формализуемых процессов информационного противоборства. Сама модель строится на основе использования интеллектуальных методов, учитывающих суждения специалистов и предоставляющих окончательный результат в виде простых операций над неопределенностью, неточностью и размытостью событий информационной безопасности (теория нечетких множеств, лингвистическая неопределенность, нечеткая логика).

ЛИТЕРАТУРА

1. Дунин В.С. Состояние и перспективы развития функциональных подсистем комплексной автоматизированной интеллектуальной системы «Безопасный город» // Общественная безопасность, законность и правопорядок в III тысячелетии: сборник материалов Международной научно-практической конференции. — Ч. 3. Естественные, математические и технические науки. — Воронеж: Воронежский институт МВД России, 2010. — С. 33—40.

2. Дунин В.С. К вопросу о построении модели управления подсистемы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город» // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сб. материалов Всероссийской научно-практической конференции курсантов, слушателей, студентов, адъюнктов и молодых специалистов. — Воронеж: Воронежский институт МВД России, 2011. — С. 91 — 92.

3. Информационная безопасность открытых систем: учебник для вузов: в 2 т. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.]. — М.: Горячая линия-Телеком, 2006. — 536 с.: ил.

4. Машкина И.В., Гузаиров М.Б. Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Приложение к журналу «Информационные технологии». — 2008. — №7. — С.32.

5. Национальный стандарт Российской Федерации. Информационная технология. Практические правила управления информационной безопасностью: ГОСТ ИСО/МЭК 17799 — 2005 г.

6. Куликов В.В. Дискретная математика: учеб. пособ. — М.: РИОР, 2007. — 174 с.

7. Дунин В.С., Бокова О.И., Хохлов Н.С. Построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД на основе нечеткой нейронной продукционной сети // Вестник Воронежского института МВД России. — 2011. — №2. — С. 48—58.

СВЕДЕНИЯ ОБ АВТОРАХ СТАТЬИ:

Дунин Вадим Сергеевич. Преподаватель кафедры информационного и технического обеспечения ОВД. Адъюнкт заочной формы обучения кафедры инфокоммуникационных систем и технологий Воронежского института МВД России.

Дальневосточный юридический институт МВД России.

E-mail: dvs_82@mail.ru

Россия, 680052, Хабаровск, переулок Казарменный, 15. Тел. 8(4212) 29-47-86.

Хохлов Николай Степанович. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, профессор. Академик РАЕН.

Воронежский институт МВД России.

E-mail: nikolayhohlov@rambler.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. 8(473) 262-33-85.

DuninVadim Sergeevich. The lecturer of the chair of Information and Technical Maintenance of the Law Inforcement Agencies.The post-graduate cadet of correspondence form education of the chair of Infocommunication Systems and Technologies of Voronezh Institute of the Ministry of the Interior of Russia.

Far East Law Institute of the Ministry of the Interior of Russia.

Work address: Russia, 680052, Khabarovsk, Kazarmenny lane, 15. Tel. 8(4212) 29-47-86.

Khokhlov Nikolay Stepanovich. Professor of the chair of Infocommunication Systems and Technologies. Doctor of technical sciences, professor, academician of the Russian Academy of Natural Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8(473) 262-33-85.

Ключевые слова к статье: нечеткая нейронная продукционная сеть; нейронечеткая классификация; адаптивная система защиты информации; инфокоммуникационная система; оценка эффективности; показатель защищенности.

Key words: rule-based fuzzy neural network; neuro-fuzzy classification; adaptive system of information protection; infocommunication system; evaluation of the efficiency; measure of protection.

УДК 621.391

Н.В. Волынкина,
кандидат педагогических наук, доцент,
ВАИУ (г. Воронеж)

С.А. Лещенко,
кандидат педагогических наук, доцент,
ВИ ФСИН

МАТЕМАТИЧЕСКИЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ ИНФОЛИНГВИСТИЧЕСКОЙ СИСТЕМЫ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНО-ТВОРЧЕСКИХ СПОСОБНОСТЕЙ КУРСАНТОВ В УЧЕБНЫЙ ПРОЦЕСС ВЕДОМСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

IMPLEMENTATION EFFICIENCY MATHEMATIC ANALYSIS OF THE INFOLINGUISTIC SYSTEM OF THE CADETS' INTELLECTUAL AND CREATIVE ABILITIES DEVELOPMENT IN THE TRAINING COURSE OF A DEPARTMENTAL EDUCATIONAL INSTITUTION

Осуществлено доказательство эффективности внедрения инфолингвистической системы развития интеллектуально-творческих способностей курсантов в учебный процесс ведомственного образовательного учреждения методами математической статистики и табличной интерпретации данных.

The article deals with the implementation efficiency proof of the infolinguistic system of the cadets' intellectual and creative abilities development in the training course of a departmental educational institution by methods of mathematic statistics and table interpretation of the data.

В настоящее время актуализируется потребность в высококлассном специалисте для правоохранительных органов, способном принимать эффективные, нестандартные решения в быстроменяющихся условиях современной жизни. В образовательный процесс высшего учебного заведения в целом и в процесс обучения иностранному языку в частности активно внедряются системотехнические комплексы. Все это инициирует создание нового направления в педагогической науке, открывающего инфолингвистический путь развития интеллектуально-творческих способностей — *инфолингвистиче-*

ской системы развития интеллектуально-творческих способностей курсантов ведомственного образовательного учреждения.

Инфолингвистический путь предполагает интеграцию информационных и лингвистических (иноязычных) ресурсов. *Инфолингвистическая система развития интеллектуально-творческих способностей (ИЛС РИТС)* курсантов — это интегрированный комплекс взаимосвязанных элементов — цели, содержания, форм и методов учебной деятельности, — основанный на оптимальном использовании информационных и лингвистических (иноязычных) ресурсов, реализующий концептуальный аспект и процессуальную деятельность при диалектическом взаимодействии субъектов образовательного процесса и направленный на развитие интеллектуально-творческих способностей духовно-нравственной личности, готовой выстраивать и эффективно реализовывать свою жизненную стратегию в условиях развития информатизации общества и новых наукоемких технологий.

Концептуальной основой построения ИЛС РИТС является направленность системы на развитие интеллектуально-творческих способностей «вторичной языковой IT-личности», обладающей свойствами системно-прогностического мышления и методическим инструментарием творческого решения проблемы. Системообразующим фактором является дисциплина «Иностранный язык», задающая стратегию деятельности, ориентированной на развитие интеллектуально-творческих способностей молодого человека в процессе его вхождения в информационное социокультурное пространство.

Ведущая идея инфолингвистической системы состоит в том, что эффективное развитие интеллектуально-творческих способностей курсантов ведомственного образовательного учреждения обеспечивает комплексно-интегрированный ресурсный потенциал информационного социокультурного пространства, профильных дисциплин, учебной дисциплины «Иностранный язык» в неязыковом вузе, а также высокоэффективные методы развития интеллектуально-творческих способностей, в том числе методы теории решения изобретательских задач (ТРИЗ).

Инновационная система, как любое сложное педагогическое явление, требует математически однозначного подтверждения эффективности своего внедрения в образовательный процесс высшего учебного заведения. В связи с этим был проведен глубокий *комплексный, уровневый* и *сравнительный* анализ с целью накопления эмпирических данных в опытно-экспериментальной работе. Комплексный анализ основан на определении показателей развития интеллектуально-творческих способностей согласно сформулированным критериям. Уровневый анализ предполагает выявление уровня развития интеллектуально-творческих способностей по каждому из критериев. Сравнительный анализ заключается в сопоставлении уровней развития интеллектуально-творческих способностей в экспериментальной и контрольной группах.

В процессе опытно-экспериментальной работы в Краснодарском университете МВД России были проведены замеры по выявлению уровня развития интеллектуально-творческих способностей испытуемых по четырём критериям (мотивационно-когнитивному, компетентностному, оперативно-процессуальному и рефлексивно-оценочному). По методике В. П. Беспалько был рассчитан коэффициент развития интеллектуально-творческих способностей каждого курсанта по каждому критерию в экспериментальных и контрольных группах до и после проведения эксперимента. Полученные результаты были распределены по трем уровням развития интеллектуально-творческих способностей (креативно-устойчивый (высокий), потенциально-продуктивный (средний), адаптационно-репродуктивный (низкий)), рассчитана частота распределения уровня развития ИТС по сумме четырёх критериев по каждому из уровней в экспери-

ментальных и контрольных группах до и после эксперимента, проведен сравнительный анализ полученных результатов и доказана их статистическая значимость по критерию χ^2 Пирсона.

Измерение проводилось с использованием диагностического пакета по каждому критерию. Максимальное количество баллов по каждому критерию составляет 100, следовательно, максимальное количество по всем четырем критериям — 400 баллов по аналогии с методикой Хекхаузена для исследования мотивации достижений или в тесте фрустрационной толерантности Розенцвейга.

С использованием методики В.П. Беспалько был получен коэффициент развития интеллектуально-творческих способностей ($К_{Pi}$):

$$К_{Pi}=\frac{\sum_{i=1}^{q} q_i}{P_i}, \quad (1)$$

где $\sum_{i=1}^{q} q_i$ — сумма баллов при тестировании по *i*-му критерию;

P_i — максимальное количество баллов по *i*-му критерию (в нашем случае $P_i = 100$).

В экспериментальной группе развитие интеллектуально-творческих способностей испытуемых осуществлялось по инновационной технологии в рамках инфолингвистической системы, а в контрольной группе — по традиционным технологиям.

Результаты расчета $К_{Pi}$ по каждому критерию распределены на трем уровням:

$0,8<К_р\leq 1,0$ — креативно-устойчивый (высокий)

$0,5\leq К_р\leq 0,8$ — потенциально-продуктивный (средний)

$0<К_р<0,5$ — адаптационно-репродуктивный (низкий)

В эксперименте, проведенном в данном ведомственном образовательном учреждении, количество значений по каждому критерию распределилось, как показано в табл. 1.

Таблица 1

Распределение количества значений (частота) результатов измерения развития ИТС по каждому критерию в контрольной и экспериментальной группах

Срезы	Группы	Критерии	Креативно-устойчивый (высокий)	Потенциально-продуктивный (средний)	Адаптационно-репродуктивный (низкий)
До	Эксп.	Мотивационно-когнитивный	18	110	72
		Компетентностный	17	112	71
		Оперативно-процессуальный	16	109	75
		Рефлексивно-оценочный	18	107	75
	Контр.	Мотивационно-когнитивный	16	111	73
		Компетентностный	18	110	72
		Оперативно-процессуальный	18	108	74
		Рефлексивно-оценочный	18	103	79
После	Эксп.	Мотивационно-когнитивный	23	137	40
		Компетентностный	21	134	45
		Оперативно-процессуальный	19	135	46
		Рефлексивно-оценочный	20	136	44
	Контр.	Мотивационно-когнитивный	17	114	69
		Компетентностный	19	116	65
		Оперативно-процессуальный	18	110	72
		Рефлексивно-оценочный	19	107	74

Частоты распределения количества значений результатов измерения развития ИТС по всем критериям в экспериментальной ($f_{эj}$) и контрольной ($f_{кj}$) группах до и после эксперимента определяются по формулам:

$$f_{эj} = \frac{\sum_{i=1}^{n} n_{эij}}{n_э}, \quad (2)$$

где $n_{эij}$ — результат распределения по уровням количества значений результатов измерения развития ИТС по каждому критерию в экспериментальной группе; $n_э$ — количество критериев ($n_э$=4),

$$f_{кj} = \frac{\sum_{i=1}^{n} n_{кij}}{n_к}, \quad (3)$$

где $n_{кij}$ — результат распределения по уровням количества значений (частота) результатов измерения развития ИТС по каждому критерию в контрольной группе; $n_к$ — количество критериев ($n_к$=4).

Частоты распределения количества значений результатов измерения развития ИТС по всем критериям в экспериментальной и контрольной группах до и после эксперимента приведены в табл. 2.

Таблица 2

Частоты распределения количества значений результатов измерения развития ИТС в контрольной и экспериментальной группах по всем критериям

Срезы	Группа	Уровни			Всего
		высокий	средний	низкий	
Предэкспериментальный	Экспериментальная	17,25	109,50	73,25	200
	Контрольная	17,50	108,00	74,50	200
Постэкспериментальный	Экспериментальная	20,75	135,50	43,75	200
	Контрольная	18,25	111,75	40,00	200

На основании критерия χ^2 Пирсона сравнивались результаты тестирования в экспериментальной и контрольной группах до реализации эксперимента. Выдвигались две гипотезы:

H_0 — распределение результатов тестирования в экспериментальной и контрольной группах не имеет существенных различий;

H_1 — распределение результатов тестирования в экспериментальной и контрольной группах имеет существенные различия.

Таблица 3 демонстрирует уровни оценок (разряды) и количество результатов, попавших в каждый уровень, — соответствующие им частоты f_j. Для экспериментальной группы значения $f_{эj}$ фиксируются в первом столбце, а для контрольной группы $f_{кj}$ — во втором. В третьем столбце отражены разности между частотами экспериментальной и контрольной групп.

Далее было определено число степени свободы по формуле:

$$\nu = k - 1, \quad (4)$$

где k — количество разрядов признака. Полученные разности были возведены в квадрат и внесены в четвертый столбец, квадраты разностей были разделены на частоту контрольной группы, и результаты занесены в пятый столбец, затем суммировалось значение пятого столбца. Полученная сумма обозначалась как $\chi^2_{эксп}$.

Далее были определены критические значения для данного числа степени свободы ν. Если $\chi^2_{эксп}$ меньше критического значения, то расхождение между распределениями статистически недостоверны. Если $\chi^2_{эксп}$ равно или превышает критическое значение, то расхождение между распределениями статистически достоверно.

Таблица 3

Расчет коэффициента Пирсона χ^2 до эксперимента

Уровни	$f_{эj}$	$f_{кj}$	$f_{эj} - f_{кj}$	$(f_{эj} - f_{кj})^2$	$\frac{(f_{эj} - f_{кj})^2}{f_{кj}}$
Креативно-устойчивый (высокий)	17,25	17,50	– 0,25	0,06	0,004
Потенциально-продуктивный (средний)	109,50	108,00	1,50	2,25	0,021
Адаптационно-репродуктивный (низкий)	73,25	74,50	–1,25	1,56	0,021
Всего	200	200	0		0,045

Алгоритм вычислений, таким образом, выражается формулой:

$$\chi^2 = \sum_{j=1}^{k} \frac{(f_{эj} - f_{кj})^2}{f_{кj}} \quad , \qquad (5)$$

где $f_{эj}$ — частота распределения уровня оценок по всем критериям для экспериментальной группы по j-му разряду признака до эксперимента, $f_{кj}$ — частота распределения уровня оценок по всем критериям для контрольной группы по j-му разряду признака до эксперимента. Определив по табличным значениям, что

$$\chi^2_{кр} = \begin{cases} 5{,}991\ (P \le 0{,}05) \\ 9{,}210\ (P \le 0{,}01), \end{cases}$$

строим «ось значимости». Чем больше отклонение частот экспериментальной группы от частот контрольной группы, тем больше будет величина χ^2, поэтому зона значимости располагается справа, а зона незначимости — слева (рис. 1).

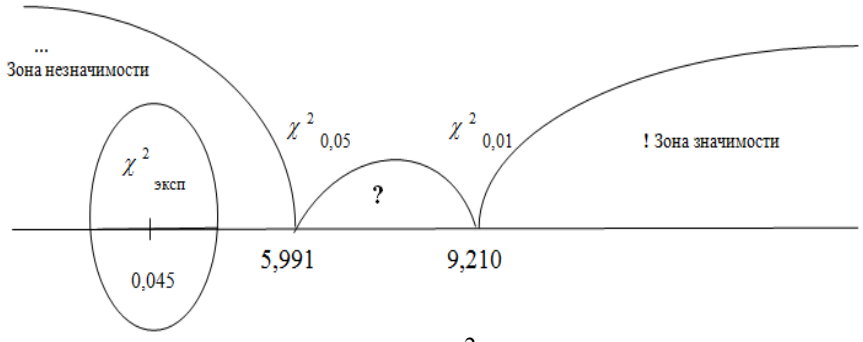


Рис. 1. Положение коэффициента Пирсона χ^2 на «оси значимости» до эксперимента

Из рисунка видно, что $\chi^2_{эксп} < \chi^2_{кр}$, следовательно, принимается H_0.

На основании данного расчета можно сделать вывод, что до начала эксперимента контрольная и экспериментальная группы статистически не отличались друг от друга по результатам предэкспериментального среза.

Далее был проведен аналогичный расчет по результатам измерений, проведенных после эксперимента. Выдвигались две гипотезы:

H_0 — распределение результатов тестирования в экспериментальной и контрольной группах не имеет существенных различий;

H_1—распределение результатов тестирования в экспериментальной и контрольной группах имеет существенные различия.

$f_{эj}$ — частота распределения уровня оценок по всем критериям для экспериментальной группы по j-му разряду признака после эксперимента,

$f_{кj}$ — частота распределения уровня оценок по всем критериям для контрольной группы по j-му разряду признака после эксперимента (табл. 4).

Таблица 4

Расчет коэффициента Пирсона χ^2 после эксперимента

Уровни	$f_{эj}$	$f_{кj}$	$f_{эj} - f_{кj}$	$(f_{эj} - f_{кj})^2$	$\frac{(f_{эj} - f_{кj})^2}{f_{кj}}$
Креативно-устойчивый (высокий)	20,75	18,25	2,50	6,25	0,342
Потенциально-продуктивный (средний)	135,50	111,75	23,75	564,06	5,048
Адаптационно-репродуктивный (низкий)	43,75	70,00	–26,25	689,06	9,844
Всего	200	200	0		15,234

«Ось значимости» приведена на рис. 2, из которого видим, что $\chi^2_{эксп} > \chi^2_{кр}$, следовательно, принимается H_1.

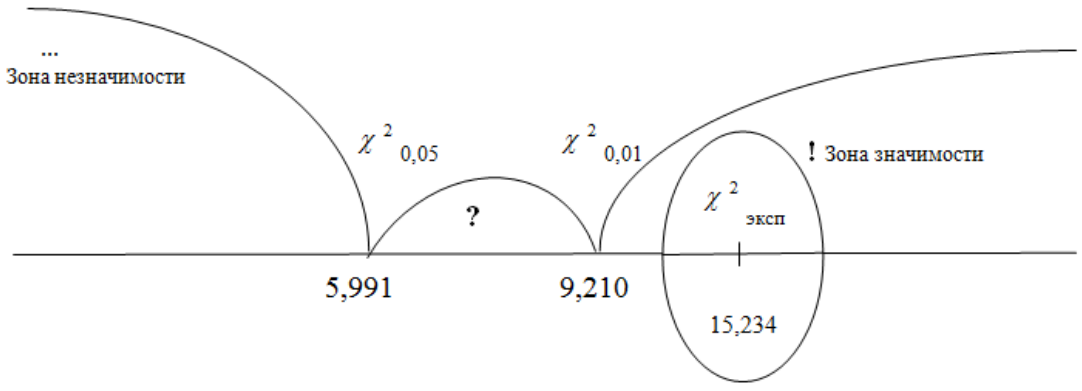


Рис. 2 .Положение коэффициента Пирсона χ^2 на «оси значимости» после эксперимента

На основании произведенных расчетов можно сделать вывод, что после завершения эксперимента контрольная и экспериментальная группы статистически отличались друг от друга по результатам постэкспериментального среза.

Была проведена ***качественная*** оценка и доказано, что результаты тестирования, проведенного в экспериментальной группе, отличались от результатов тестирования в контрольной группе в ***положительную*** сторону. Для этого каждому значению частоты в каждом из разрядов было присвоено соответствующее количество оценочных баллов. Значениям, соответствующим «высоким» результатам тестирования, был присвоен 1 балл, «средним» — 0,5 балла, «низким» — 0 баллов. Среднее арифметическое значение баллов в экспериментальной и контрольной группах было выведено по формуле:

$$\text{Р} = \frac{\sum_{j=1}^{n}(n_j \times b_j)}{\sum_{j=1}^{n} n_j}, \quad (6)$$

где b_j — соответствующее количество оценочных баллов для каждого уровня.

$$\text{Р}_э = 0{,}4425,\ \text{Р}_к = 0{,}3706,$$

$$0{,}4425 > 0{,}3706, \text{ т.е. } \text{Р}_э > \text{Р}_к.$$

В табл. 5 показана динамика измерения уровня развития интеллектуально-творческих способностей испытуемых в результате внедрения инфолингвистической системы в образовательный процесс Краснодарского университета МВД России. Для её расчёта используется формула:

$$\Delta = \frac{(f_{после} - f_{до})}{f_{до}}, \quad (7)$$

где Δ — относительное изменение числа соответствующих распределений;

$f_{после}$ и $f_{до}$ — соответственно частоты распределения уровня оценок по всем критериям до и после эксперимента.

Из табл. 5 видно, что внедрение инновационной системы развития интеллектуально-творческих способностей в образовательный процесс дает ощутимый результат в виде увеличения количества испытуемых, имеющих креативно-устойчивый уровень интеллектуально-творческих способностей, на 16% по сравнению с традиционным подходом, увеличение процента курсантов с потенциально-продуктивным уровнем развития ИТС на 20,3% и уменьшение числа молодых людей с адаптационно-репродуктивным уровнем развития ИТС на 34,2%.

Таблица 5

Динамика изменения уровня развития интеллектуально-творческих способностей испытуемых (в %)

Уровни	Экспериментальная группа	Контрольная группа	Разница показаний в контрольной и экспериментальной группах
Креативно-устойчивый (высокий)	20,3	4,3	16,0
Потенциально-продуктивный (средний)	23,7	3,5	20,3
Адаптационно-репродуктивный (низкий)	–40,3	–6,0	–34,2

Таким образом, анализ полученных количественных и качественных изменений уровня развития интеллектуально-творческих способностей в контрольной и экспериментальной группах дает нам основание утверждать, что комплекс организационно-педагогических условий, реализованных в Краснодарском университете МВД России, действительно способствует положительной динамике формирования интеллектуально-творческих способностей курсантов, а разработанная инфолингвистическая система развития интеллектуально-творческих способностей обеспечивает успешность данного процесса.

СВЕДЕНИЯ ОБ АВТОРАХ СТАТЬИ:

Волынкина Наталия Валериевна. Доцент кафедры иностранных языков. Кандидат педагогических наук, доцент.

Военный авиационный инженерный университет (г. Воронеж).

E-mail: Volynkina_n@mail.ru

Россия, 394064, Воронеж, ул. Старых Большевиков, 54 а. Тел. 8(473)226-60-13.

Лещенко Светлана Александровна. Начальник организационно-научного и редакционного отдела. Кандидат педагогических наук, доцент.

ФКОУ ВПО Воронежский институт ФСИН России.

E-mail: svt773311@hotmail.com

Россия, 394072, г. Воронеж, Иркутская, 1а. Тел. 8(473)2260-68-11.

Volynkina Natalia Valerievna. Assistant professor at the chair of Foreign Languages. Ph.D. (Pedagogics), assistant professor.

Military Air Force Engineering University (Voronezh).

Work address: Russia, 394064, Voronezh, Staryh Bolshevikov Str., 54 a. Tel. 8(473)226-60-13.

Leshchenko Svetlana Alexandrovna. The head of the scientific and editor department. Ph. D. (Pedagogics), assistant professor.

Institute of the Penitentiary Service of Russian Federation (Voronezh).

Work address: Russia, 394064, Voronezh, Irkutskaya Str., 1a. Tel. 8(473)2260-68-11.

Ключевые слова к статье: инфолингвистическая система; интеллектуально-творческие способности; математическая статистика.

Key words: the infolinguistic system; intellectual and creative abilities; mathematic statistics.

УДК 517:81:355.233

Н.В. Филатов,
Управление связи Департамента информационных технологий, связи и защиты информации МВД России

А.В. Конюхов,
Управление связи Департамента информационных технологий, связи и защиты информации МВД России

РАЗРАБОТКА АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ В РАМКАХ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД»

DEVELOPMENT OF ARCHITECTURE IN THE INFORMATION SYSTEMS HARDWARE SOFTWARE COMPLEX "SAFE CITY"

Приводится анализ традиционной архитектуры информационной системы на базе хранилищ данных. Осуществляется разработка новой архитектуры для использования в аппаратно-программном комплексе «Безопасный город». Предлагаются концептуальные решения по построению информационных систем применительно к задачам органов внутренних дел.

The article is carried out analysis of the traditional architecture of information systems based on the data warehouse. A new architecture for use in hardware-software system "Safe city" is proposed. Conceptual solutions for building information systems in relation to the tasks of the Law Inforcement Agencies are offered.

По поручению Президента Российской Федерации от 26 сентября 2005 года «О создании государственной системы профилактики правонарушений МВД России» в ряде МВД, ГУ МВД, У МВД России по субъектам Российской Федерации ведутся работы по созданию технических систем охраны общественного порядка и обеспечению безопасности в рамках аппаратно-программного комплекса «Безопасный город».

АПК «Безопасный город» — комплекс технических, программных, инженерных и иных материальных средств, используемых совместно органами государственной власти, уполномоченными службами и подразделениями федеральных органов исполнительной власти в целях обеспечения профилактики, пресечения, расследования и раскрытия преступной и иной противоправной деятельности, поддержания обществен-

ной безопасности и охраны общественного порядка на территориях населённых пунктов городского типа.

В состав АПК входят: подсистема видеонаблюдения, подсистема экстренной связи «Гражданин-полиция», спутниковые навигационно-мониторинговые системы ГЛОНАСС или ГЛОНАСС/GPS.

Используемые системы не только предоставляют информацию в режиме реального времени о ситуации в городе, но и позволяют обеспечивать хранение данных для последующей аналитической обработки с целью оптимизации как осуществления охраны общественного порядка и обеспечения безопасности, так и работы самого АПК. Существующие методы хранения и анализа данных [1, 2] предлагают различные подходы к построению информационных и информационно-аналитических систем, основанных на использовании хранилищ данных, но часто не учитывают задачи и специфику работы органов внутренних дел.

Существующие фактические стандарты построения корпоративных информационно-аналитических систем, основаны на концепции хранилища данных [1, 3]. Эти стандарты опираются на современные исследования и общемировую практику создания хранилищ данных и аналитических систем. В общем виде архитектура корпоративной информационно-аналитической системы описывается схемой с тремя выделенными слоями (рис.1):

извлечение, преобразование и загрузка данных,

хранение данных,

анализ данных (рабочие места пользователей).

Технология функционирования системы состоит в следующем. Данные поступают из различных внутренних транзакционных систем, от подчинённых структур, от внешних организаций в соответствии с установленным регламентом, формами и макетами отчётности. Вся эта информация проверяется, согласуется, преобразуется и помещается в хранилище и витрины данных. После этого пользователи с помощью специализированных инструментальных средств получают необходимую им информацию для построения различных табличных и графических представлений, прогнозирования, моделирования и выполнения других аналитических задач.

Однако в рамках развёртывания АПК «Безопасный город» данная архитектура обладает рядом недостатков:

1. В качестве хранилища данных в настоящее время используется реляционная база данных, работающая под управлением достаточно мощной реляционной СУБД. Однако реляционные базы данных показывают низкую эффективность и производительность при работе с нетипичными видами данных — видео, документы, геоинформационные данные. В связи с этим необходимо включение в слой хранения данных (рис. 1) нереляционных баз данных, удовлетворяющих следующим требованиям:

- гарантировать высокую скорость обработки запросов к нетиповым видам данных;
- предоставлять простой доступ к хранящимся данным;
- обеспечивать проведение транзакций с высоким уровнем надёжности и поддержки;
- поддерживать наиболее широко используемые платформы и языки создания программных средств — Java, Erlang, C++.

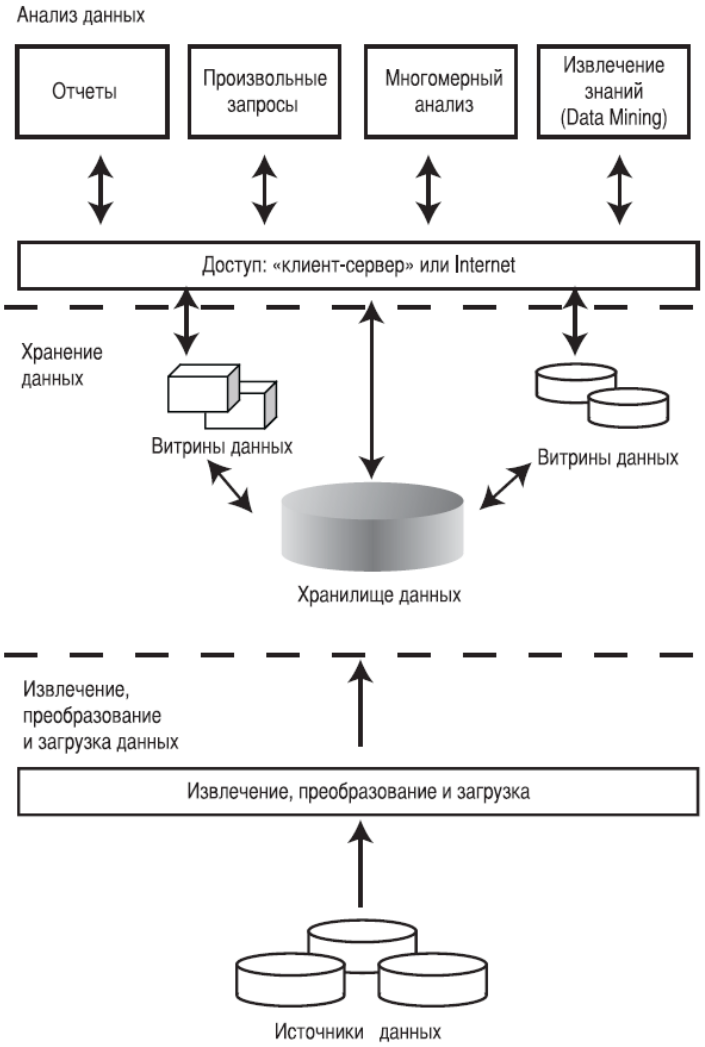


Рис. 1. Традиционная архитектура информационно-аналитической системы

2. В хранилище данных поступают значимые, проверенные, согласованные, непротиворечивые и хронологически целостные данные, которые с достаточно высокой степенью уверенности можно считать достоверными. При этом на осуществление процедур извлечения и преобразования данных (рис. 1) тратится некоторое время, что приводит к отставанию «реальной» обстановки от «наблюдаемой», в то время как для осуществления охраны общественного порядка, обязательным является наблюдение в реальном времени, а желательным — возможность предугадывать изменение состояния обстановки с целью предупреждения правонарушений.

3. Поскольку использование АПК «Безопасный город» осуществляется не только органами внутренних дел, но и другими органами государственной власти, уполномоченными службами и подразделениями федеральных органов исполнительной власти, то способ доступа «клиент-сервер» традиционной архитектуры может оказаться «узким горлышком» и приводить к низкой производительности всей системы в целом. Связано это с тем, что при осуществлении электронного межведомственного взаимо-

действия могут возникать запросы к хранилищу (например, выгрузка видеоданных), требующие, с учётом типов имеющихся данных, высокой пропускной способности канала связи.

В связи с этим потребуется обеспечивать не только «клиент-серверный» вид доступа к хранилищу данных, но и использование других способов: локальный «клиент-приложение-сервер» или распределённый «клиент-приложение-сервер».

Независимо от выбранного вида доступа в составе СУБД необходимо предусмотреть развитые средства ограничения доступа, обеспечить повышенный уровень надёжности и секретности.

4. Архитектурой не предусмотрен единый интерфейс обмена данными (ЕИОД) с хранилищами других ведомств, что ограничивает возможности информационного взаимодействия. Наличие единого интерфейса (иногда его называют шиной передачи данных) позволяет в общем случае не только упростить процедуры обмена на уровне хранения данных между ведомствами, но и значительно облегчить и ускорить процесс разработки программных средств.

5. Подсистемы, входящие в состав АПК, в принципе могут обладать некоторой интеллектуальной способностью анализа отслеживаемых процессов. Например, обрабатывая видео- и сенсорную информацию, подсистема видеонаблюдения способна анализировать и распознавать ситуации нарушения общественной безопасности (оставленный предмет, беспорядки, драку, бегущего человека, проезд на красный свет, остановку транспортного средства в неположенном месте). В соответствии с этим в архитектуре необходимо предусмотреть возможность реагирования на нештатные ситуации, минуя промежуточные уровни. Таким образом, осуществление мониторинга работы подсистем и их сообщений на нештатные ситуации позволит уменьшить время реакции, что в общем случае может привести к уменьшению размеров последствий совершаемых правонарушений.

6. В архитектуре отсутствует обратная связь с уровня анализа данных к источникам данных, т.е. система является «пассивным» наблюдателем. Однако в используемых в составе АПК подсистемах имеются возможности по управлению оконечными устройствами (например, камерами наблюдения, нарядами полиции и др.), что позволяет формировать потоки интересующей с точки зрения обеспечения безопасности информации.

С учётом вышесказанного предлагается архитектура информационной системы в составе АПК «Безопасный город» (рис. 2).

Таким образом, в предлагаемой архитектуре информационной системы предполагается устранение недостатков, присущих традиционной архитектуре на базе хранилища данных, при одновременной поддержке решения специфичных задач органов внутренних дел в рамках АПК «Безопасный город». Осуществление управления подсистем АПК и непосредственный мониторинг предоставляемой ими информации позволит более качественно и эффективно решать задачи охраны общественного порядка и обеспечения безопасности граждан.

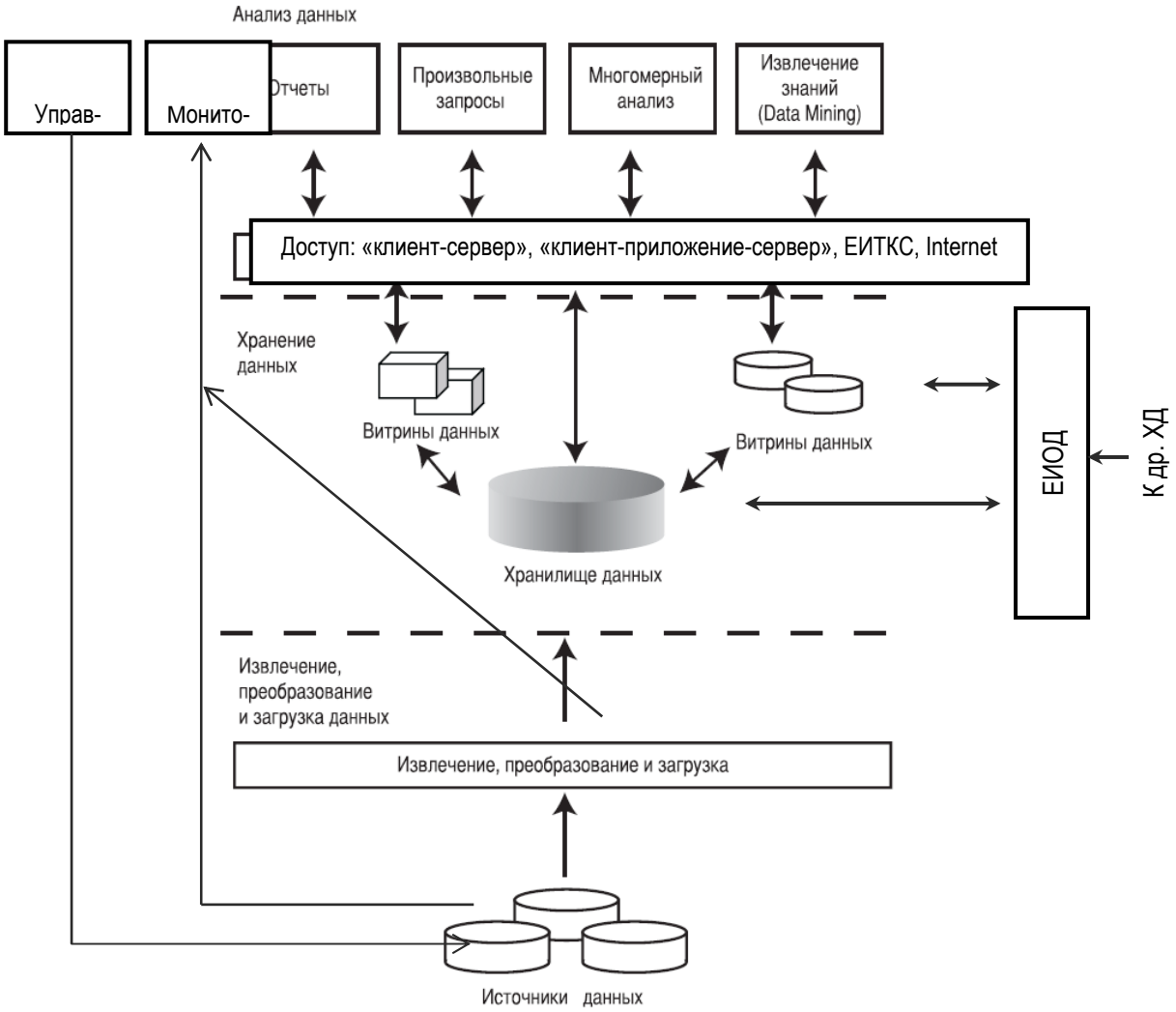


Рис. 2. Предлагаемая архитектура информационной системы
в составе АПК «Безопасный город»

ЛИТЕРАТУРА

1. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / А.А. Барсегян [и др.]. — 2-е изд., перераб. и доп. — СПб.:БХВ-Петербург, 2007. — 384 с.

2. Mattison R. Data warehousing and data mining for telecommunications. — London: ACSL, 1997. —282 с.

3. Хранилища данных и аналитические системы: Технологии и инструментальные средства корпорации Oracle / www.oracle.com/ru

СВЕДЕНИЯ ОБ АВТОРАХ СТАТЬИ:

Филатов Николай Владимирович. Начальник Управления связи.
Департамент информационных технологий, связи и защиты информации МВД России.
E-mail: filatov.n@mail.ru
Россия, 119049, г. Москва, ул. Житная, 16. Тел. (495) 667-80-33.

Конюхов Александр Викторович. Начальник отделения организации радиорелейной и проводной связи отдела организации связи Управления связи.
Департамент информационных технологий, связи и защиты информации МВД России.
E-mail: oos_mvd@mail.ru
Россия, 119049, г. Москва, ул. Житная, 16. Тел. (495) 667-53-69.

Filatov Nikolay Vladimirovich. Head of the Communications Agency of Department of Information Technologies, Communications and Information Protection of the Ministry of the Interior of Russia.
Work address: Russia, 119049, Moscow, Zhitnaya Str., 16. Tel. (495) 667-80-33.

Konyukhov Alexander Victorovich. Head of section of organization of microwave and wireline communications of division of the Communications Agency of Department of Information Technology, Communications and Information Protection of the Ministry Interior of Russia.
E-mail: oos_mvd@mail.ru
Work address: Russia, 119049, Moscow, Zhitnaya Str., 16. Tel. (495) 667-53-69.

Ключевые слова: информационные системы; хранилища данных; безопасный город.

Key words: information systems; data warehouse; safe city.

УДК 519.7

О.А. Черникова,
ПП №9 ОП № 3 УМВД России по г. Воронежу

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ РАДИОСВЯЗИ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧИХ ЧАСТОТ

MATHEMATIC MODEL OF RADIO SYSTEMS WITH PSEUDO-REARRANGEMENT OF THE OPERATION FREQUENCY

Показана актуальность использования каналов радиосвязи в телекоммуникационных системах для решения задачи защиты передаваемой информации от преднамеренных помех. Рассмотрен режим псевдослучайной перестройки рабочей частоты как мера защиты передаваемой в телекоммуникационных системах информации от преднамеренных помех. Разработана модель телекоммуникационных систем с псевдослучайной перестройкой рабочей частоты, в которой мы постарались учесть особенности организации связи, а также особенности формирования сигналов и программ перестройки рабочей частоты применительно к перспективным средствам КВ, УКВ радиосвязи.

The article shows the relevance of the use of radio channels in telecommunications systems to address the problem of protecting transmitted information from jamming. The pseudo-mode tuning the operating frequency is considered as a measure of protection in telecommunication systems transmitted information from jamming. We elaborate a model of telecommunication systems with pseudo-rearrangement of the operation frequency, in which we tried to take into account the characteristics of the organization of communication and peculiarities of the signals and structural adjustment programs operating frequency with respect to a promising means of HF, VHF radio.

Акцент современной технической политики в сфере телекоммуникаций сделан на создании нового поколения высоконадежных систем связи. В области радиосвязи данное направление особенно ярко выразилось в реализации широкомасштабных программ создания помехозащищенных систем и средств радиосвязи, в том числе использующих режим псевдослучайной перестройки рабочих частот (ППРЧ).

По существу, реализуемый в системах радиосвязи режим ППРЧ представляет собой способ расширения спектра сигнала в пределах заданной полосы частот путем скачкооб-

разного изменения номинала несущей частоты одновременно на всех радиостанциях системы радиосвязи по априорно известному абонентам псевдослучайному закону с неисчерпываемым за время его использования периодом [4]. При этом достигаемый эффект надежности связи определяется большим объемом используемых частот, из которого осуществляется случайный для стороннего наблюдателя выбор очередной рабочей частоты, и малым временем существования сигнала на этой частоте. Это значительно усложняет контроль (обнаружение и измерение параметров) сигналов систем связи с ППРЧ и возможность постановки преднамеренных помех. А повышение разведзащищенности и помехоустойчивости, в свою очередь, повышает надежность связи.

Однако в систему связи с ППРЧ изначально заложен элемент «ненадежности». Это вызвано тем, что одновременно на одних частотах работает несколько независимых систем связи, что приводит к случайным совпадениям частот, т.е. к возникновению внутрисистемных помех, снижающих значение коэффициента готовности связи.

Сказанное обусловливает актуальность разработки математической модели функционирования систем связи с ППРЧ в условиях радиоэлектронного конфликта, проведения исследования их надежности и выработки предложений по повышению надежности связи. Целью данной статьи является разработка математической модели системы радиосвязи с ППРЧ.

Ключевыми элементами радиостанций, реализующих режим ППРЧ, являются генератор псевдослучайной последовательности (ПСП) и блок синхронизации. Генераторы ПСП управляют синтезаторами частоты на передающей и приемной сторонах системы связи. Для их синхронизации производятся установка исходной кодовой комбинации (базового ключа) и одновременный запуск генераторов ПСП на всех радиостанциях системы радиосвязи по синхросигналу управляющей станции. Синхросигнал содержит синхрослово, представляющее собой кодовую комбинацию для загрузки генераторов ПСП, и маркер типа сообщения для автоматического опознавания синхросигнала. Синхросигналы передаются на рабочих частотах и внешне не отличаются от текущей информации.

Исходными данными для организации связи в режиме ППРЧ являются:

- адресная группа частот (АГЧ) — подмножество рабочих частот, используемых для ППРЧ;

- код идентификации сети, задающий частоту, на которой работает радиостанция в режиме фиксированной настройки частоты и с которой начинается ППРЧ;

- «время дня» — время начала ППРЧ;

- «слово дня», или транзективная переменная, — правило соответствия частот АГЧ и кодовых комбинаций, формируемых генератором ПСП.

Эти данные получили название «*ключевых переменных*» [3].

Повышение устойчивости систем радиосвязи с ППРЧ к воздействию систем радиоконтроля и радиопротиводействия может быть достигнуто увеличением используемых объемов АГЧ K, поддиапазонов ППРЧ $F_{ппрч}$, скорости ППРЧ $v_{ппрч}$ и уменьшением времени излучения на частоте $t_и$. Это приводит к увеличению стоимости средств, что объясняет варьирование значений названных параметров в широких пределах: $K=4…2400$, $F_{ппрч}=0{,}016…200$МГц, $v_{ппрч}=2…38500$ск/с, $t_и=6{,}4$мкс…$0{,}5$с.

Частотные последовательности, используемые в системах радиосвязи с ППРЧ, формируются на основе алгоритма [4]:

$$\{i\} \xrightarrow{A} \{f_i\} \,/\, i \in N, f_i \in F = \left\{f^{\langle 0\rangle}, f^{\langle 1\rangle}, ..., f^{\langle K-1\rangle}\right\}, T_{ппрч} > T_{исп},$$

где $\{i\}$ — ряд натуральных чисел; A — алгоритм формирования частотной последовательности $\{f_i\}$; N — множество натуральных чисел; F — адресная группа частот; $T_{ппрч}$ — период ППРЧ; $T_{исп}$ — время использования частотной последовательности.

ППРЧ-сигнал может быть описан следующим выражением [4]:

$$s_{мн}(t) = \sum_{l}\sum_{m} S \cdot rect\left[t - (l-1)T_{ц} - (m-1)\tau_{u}\right] \cdot \sin\left[\left(w(n_l) + \Delta w_q\right) \cdot t + \Theta_0\right],$$

где $rect\left[t^* - (m-1)\cdot\tau_u\right] = \begin{cases} 1, & при \quad (m-1)\cdot\tau_u \le t^* \le m\tau_u \\ 0, & при \quad t^* < (m-1)\cdot\tau_u, t^* > m\tau_u \end{cases}$ — функция прямоугольного импульса; l — номер текущего шага программы ППРЧ, $l=1...L$; $m=1...M$, M — количество информационных символов, передаваемых на очередном шаге программы; q — номер текущего информационного символа $q=1...Q$; τ_u — длительность элементарного импульса (посылки); S — амплитуда сигнала; Θ_0 — начальная фаза сигнала; Δw_q — приращение частоты за счет модуляции q-м информационным символом; n_l — номера частот, определяющие значения номиналов частот сигнала на l-м шаге программы.

Формирование последовательности номиналов частот (ПНЧ) $\{f_i\}$ осуществляется на основе комбинационно-числового преобразования (КЧП) двоичных псевдослучайных последовательностей (ДПСП) $\{x_i\}$. Алгоритм формирования ПНЧ предполагает несколько этапов [4, 2]:

$$A = A_1 \circ A_2 \circ A_3 \circ A_4,$$

где $\circ$ — операция левой композиции функций; $A_4 : N \to D = \{0,1\}$ — правило формирования ДПСП: $\{i\} \to \{x_i \mid x_i \in D, i \in N\}$; $A_3 : D \to S = \{0,1,...,K-1\}$ — КЧП ДПСП $\{x_i\}$ в многоуровневую числовую последовательность (МЧП) $\{r_i\} : \{x_i\} \to \{r_i \mid r_i \in S, i \in N\}$, которая представляет собой последовательность десятичных чисел или их двоичных эквивалентов $\{r_i\} = \{X_{mi}\}$; $A_2 : S \to S$ — правило перенумерации элементов МЧП, определяемое транзективной переменной ключа: $\{r_i\} \to \{n_i\}$ — последовательность номеров частотных каналов (ПНК); $A_1 : S \to F$ — правило соответствия элементов ПНК $\{n_i\}$ и ПНЧ $\{f_i\}$, определяющее преобразование $\{n_i\} \to \{f_i\}$.

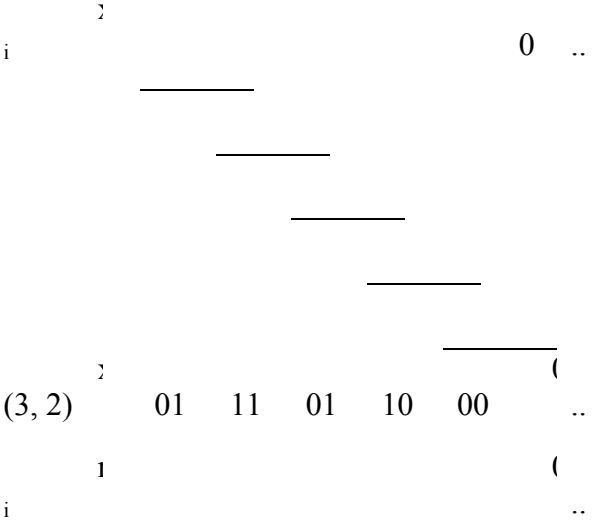
Правило A_4 определяет тип используемой двоичной ПСП и ее параметры, что, в свою очередь, однозначно определяет схему генератора ДПСП. В качестве двоичной ПСП могут использоваться как линейные (М-, Голда, Касами и др.), так и нелинейные (составные, бент-, де Брейна и др.) последовательности.

Для формирования исходной двоичной ПСП в системе радиосвязи с ППРЧ используются генераторы, построенные на регистрах сдвига, состоящих из n=(48…75) ячеек, что определяет длину формируемой ДПСП $L = 2^n - 1 = 2{,}8 \cdot 10^{14} ... 3{,}8 \cdot 10^{22}$ символов, период повторения которой, например при скорости ППРЧ, равной $v_{ппрч} = 100\,ск/с$, составит $T_{ппрч} = L / v_{ппрч} = 9 \cdot 10^5 ... 1{,}2 \cdot 10^{13}\,лет$.

Правилом A_3 является комбинационно-числовое преобразование ДПСП в МЧП, представляемое выражением

$$r_i = \sum_{k=0}^{m-1} 2^k x_{[s(i-1)+m-k]} \ ,$$

где m и s — параметры КЧП: m — параметр выборки, s — коэффициент децимации (параметр смещения).



На диаграмме показано комбинационно-числовое преобразование при m=3, s=2. В зависимости от соотношения параметров выборки и смещения выделяют три режима КЧП: 1) *скользящий* — при $s<m$; 2) *последовательных выборок* — при $s=m$; 3) *выборок с пропусками* — при $s>m$.

Элементы МЧП, с целью повышения разведзащищенности системы радиосвязи с ППРЧ, перенумеровываются в соответствии с правилом A_2, задаваемым транзективной переменной ключа. Наиболее употребимыми способами перенумерации являются инверсия отдельных символов числа $X_{(m,s)i}$ и изменение порядка следования их весовых коэффициентов:

$$n_i = \sum_{k=0}^{m-1} 2^{P_m(k)} \left(x_{[s(i-1)+m-k]} \oplus l_k \right) ,$$

где l_k=*0* или *1*, если k-й символ не инвертируется или инвертируется, соответственно; $P_m(k)$ — k-й символ перестановки P_m на множестве *{0,1,...,m–1}*; $\oplus$ — операция сложения по *mod 2*. Количество возможных вариантов правила A_2 определяется выражением

$$N_{варA_2} = 2^m m! \ ,$$

что при *m=8 (K=256)* составит более 10^7. Возможны и другие способы перенумерации элементов МЧП, в том числе и способ, заключающийся в назначении произвольного (табличного) соответствия элементов МЧП и ПНК, для которого количество возможных вариантов правила A_2 определяется выражением

$$N_{варA_2} = K! \ ,$$

что при *K=256* примерно составляет $5 \cdot 10^{507}$.

Правило A_1 определяется порядком ввода в память радиостанций с ППРЧ номиналов частот АГЧ, который может быть произвольным (задаваться оператором) или ре-

гулярным (при автоматическом выборе частот), например соответствовать равномерному возрастанию номиналов частот в заданных пределах

$$f^{\langle n \rangle} = f^{\langle 0 \rangle} + n \cdot \Delta f \ ,$$

где $f^{\langle 0 \rangle}$ — минимальное значение частоты адресной группы частот системы радиосвязи с ППРЧ, $n \in S$.

Максимальный объем адресной группы частот системы радиосвязи, программы ППРЧ которых основаны на комбинационно-числовом преобразовании двоичных ПСП, равен $K_{\max} = 2^m$.

В современных системах радиосвязи с ППРЧ в качестве оперативных мер защиты от радиоразведки и радиопротиводействия возможна полная или частичная смена ключевых данных, т.е. правил A_1, A_2 и текущего заполнения генераторов ПСП. В перспективных радиостанциях возможна реализация оперативной смены любого правила формирования частотной последовательности (A_1, A_2, A_3, A_4) в любом их сочетании.

Таким образом, режим псевдослучайной перестройки рабочей частоты является одним из наиболее эффективных методов повышения надежности в системах радиосвязи. Эффективность этого метода обусловлена сокращением времени существования сигнала на текущей рабочей частоте, что затрудняет обнаружение таких сигналов и, тем более, постановку эффективных преднамеренных помех. Однако существование целого ряда возможных способов создания помех и непрерывное совершенствование средств помех обусловливают необходимость обоснования параметров систем радиосвязи ППРЧ (время излучения сигнала на частоте, количество используемых частот, полоса частот) с целью поиска технических решений, оптимальных по показателю «надежность/стоимость».

Надежность связи характеризуется параметром *коэффициент готовности* $K_г$. Организация связи предполагает обеспечение в системе радиосвязи требуемого значения коэффициента готовности

$$K_г \geq K_{г-тр} \ .$$

В свою очередь, коэффициент готовности равен доле сигнала, не пораженной помехами

$$K_г = 1 - p_{чвк} \ ,$$

где $p_{чвк}$ — вероятность частотно-временного контакта помехи и сигнала в произвольный момент времени. Этот показатель оказывается чувствительным к значениям пространственно-временных параметров конфликтного взаимодействия средств связи и средств помех.

Обеспечение требований по надежности связи предполагает выполнение условия

$$p_{чвк} \leq p_{чвк-доп} \ ,$$

где $p_{чвк-доп} = 1 - K_{г-тр}$. Для цифровых систем радиосвязи допустимое значение вероятности частотно-временного контакта помехи и сигнала, на основании формулы полной вероятности [4], определяется выражением

$$p_{чвк-доп} = \frac{p_{ош-доп} - p_{ош-с}^{(Ш)}}{p_{ош-с}^{(П+Ш)} - p_{ош-с}^{(Ш)}} \ ,$$

где $p_{ош-с}^{(П+Ш)}$ и $p_{ош-с}^{(Ш)}$ — вероятность искажения передаваемого символа в условиях наличия и отсутствия преднамеренных помех соответственно. Допустимое для надежной радиосвязи значение вероятности искажения символа $p_{ош\text{-}доп}$ в общем случае зависит от требований, предъявляемых информационной системой, избыточности используемого кодирования, наличия перемежения символов в передаваемой информационной последовательности. Поэтому величина $p_{чвк\text{-}доп}$ может варьировать в широких пределах и должна определяться для каждой системы связи индивидуально.

Одной из эффективных мер повышения надежности в системах радиосвязи с ППРЧ является сокращение времени излучения сигнала, что в условиях ограничения частотного ресурса приводит к уменьшению количества информационных символов в передаваемом сигнале (пакете), а, следовательно, к увеличению количества сигналов (пакетов) в сообщении и времени его передачи.

В этих условиях представляет интерес поиск значений параметра «длительность излучения сигнала (информационного пакета)» $t_и$ в системе радиосвязи с ППРЧ, оптимальных как с позиции обеспечения максимальной достоверности передачи сообщения (*min* $p_{чвк}$) при ограничении времени доставки (передачи) ($T_{пер} \le T_{оц}$, где $T_{оц}$ — время оперативной ценности передаваемого сообщения) в условиях активного радиопротиводействия

$$t_и = \arg\min_{\vec{x}\in G_x} p_{чвк}(\vec{x},\vec{y},\vec{z}) \mid \vec{y}\in G_y, \vec{z}\in G_z, T_{пер} \le T_{оц} \ ,$$

так и с позиции минимизации времени доставки сообщения в условиях обеспечения требуемого качества связи

$$t_и = \arg\min_{\vec{x}\in G_x} T_{пер}(\vec{x},\vec{y},\vec{z}) \mid \vec{y}\in G_y, \vec{z}\in G_z, p_{чвк} \le p_{чвк-доп} \ ,$$

где $\vec{x},\vec{y},\vec{z}$ — векторы технических характеристик и параметров функционирования системы радиосвязи, системы радиопротиводействия и радиоэлектронной обстановки соответственно; $G_x = \{\vec{x} \mid p_{чвк}(\vec{x}) \le p_{чвк-доп}\}$, G_y, G_z — области их возможного варьирования.

Названные решения представляют собой значения *нижней* и *верхней* границ параметра «длительность излучения сигнала (информационного пакета)», в пределах которых обеспечиваются требования к надежности связи.

Таким образом, в статье представлена математическая модель систем радиосвязи с ППРЧ, предназначенная для использования при оценке надежности связи в условиях радиоэлектронного конфликта.

ЛИТЕРАТУРА

1. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. — М.: Наука, 1988. — 480 с.

2. Защита информации в телекоммуникационных системах: учебник / В.Г. Кулаков [и др.]. — Воронеж: ВИ МВД, 2002. — 300 с.

3. Клименко Н.Н. Радиостанции УКВ-диапазона: состояние, перспективы развития, особенности применения режима скачкообразного изменения частоты // Зарубежная радиоэлектроника. — 1990. — № 7. — С. 3—20; №8. — С. 20—38.

4. Обухов А.Н. Частотно-временные аспекты защиты информации в системах радиосвязи. — М.: Экслибрис-Пресс, 2008. — 212 с.

СВЕДЕНИЯ ОБ АВТОРЕ СТАТЬИ:

Черникова Ольга Александровна. Инспектор ПДН.
ПП №9 ОП № 3 УМВД России по г. Воронежу.
E-mail: ol4k@inbox.ru
Россия, 394006, г. Воронеж, Краснознаменная, 16.

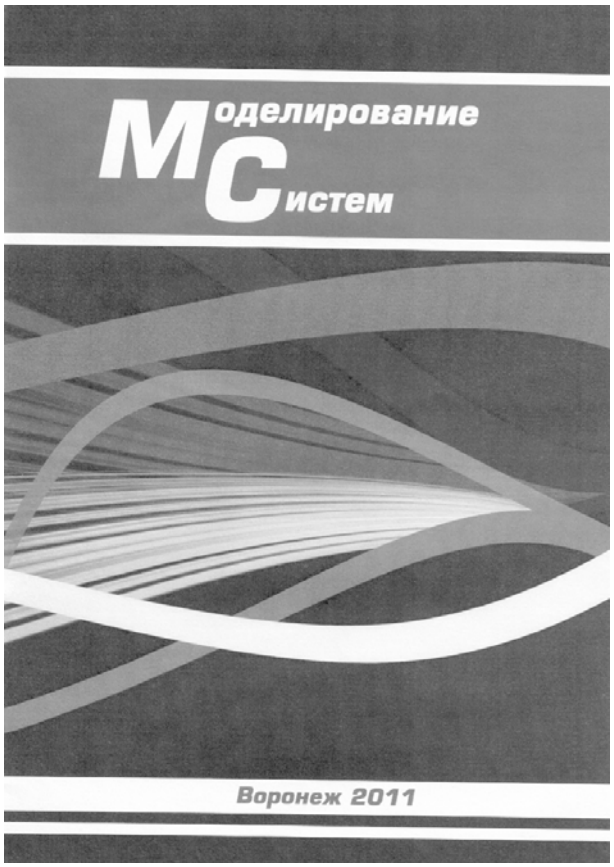
Chernikova Olga Alexandrovna. Inspector.
PD № 9 PD № 3 Department of the Ministry of the Interior of Russia in Voronezh.
Work address: Russia, 394006, Voronezh, Krasnoznamennaya Str., 16.

Ключевые слова к статье: псевдослучайная перестройка рабочей частоты; радиосвязь; телекоммуникационная система.

Key words: pseudo-rearrangement of the operation frequency; radio communication; telecommunication system.

УДК 621.382

ИЗДАНИЯ ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ



Моделирование систем: учебное пособие / В.И. Сумин [и др.]; под ред. В.И. Сумина. — Воронеж: Воронежский институт МВД России, 2011. — 222 с.

Целью данного учебного пособия является формирование теоретических знаний, практических умений и навыков в области математического моделирования, основных понятий системного подхода как методологии исследования объектов, систем, процессов. Рассматриваются вопросы, связанные с понятием системного подхода в моделировании, основами математического моделирования, получением навыков формализации и алгоритмизации функционирования устройств и систем, освоением возможностей компьютерной техники для создания и реализации моделей, выработки навыков постановки и решения информационных задач, моделирования и анализа информации в служебной деятельности сотрудников ОВД. Предназначено для курсантов и слушателей, обучающихся по специальностям 090106.65 – Информационная безопасность телекоммуникационных систем и 230102.65 – Автоматизированные системы обработки информации и управления.