ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

В.В. Меньших,
доктор физико-математических наук, профессор

А.Ю. Телков,
кандидат физико-математических наук, доцент, Воронежский государственный университет

ИСПОЛЬЗОВАНИЕ СЕТЕВОГО СЕНСОРА IPCAD ДЛЯ ПОЛУЧЕНИЯ ИСХОДНЫХ ДАННЫХ В СИСТЕМАХ ОБНАРУЖЕНИЯ АНОМАЛИЙ IP ТРАФИКА

UTILIZING NETWORK SENSOR IPCAD FOR GETTING SOURCE DATA IN SYSTEMS OF ANOMALY DETECTION OF IP TRAFFIC

Рассматривается возможность использования сетевого сенсора IPCAD для получения исходной информации с целью обработки в системах обнаружения аномалий IP трафика. Обосновываются требования к детальности получения информации. Разрабатывается методика имитационного моделирования, проводится эксперимент, обсуждаются его результаты.

Possibility of utilizing network sensor IPCAD for getting source information for processing in systems of IP traffic anomaly detection is considered. Requirements for details of information getting are founded. The methodic of imitation modelling is proposed, experiment is carry out, the results of experiment are discussed.

Введение

В настоящее время одной из глобальных проблем функционирования распределенных сетевых защищенных систем, образованных набором взаимодействующих между собой по некоторым правилам удаленных IP сетей, является проблема обнару-

жения аномалий сетевого трафика [1]. В качестве примеров можно рассматривать взаимодействующие между собой части корпоративных или ведомственных сетей, причем в первом случае, как правило, кроме внутреннего трафика между удаленными сетями существует еще и трафик между локальными сетями и сетью Интернет и т.д.

В общем виде под аномалией сетевого трафика понимают отклонение поведения сетевого трафика от «нормального» в некотором признаковом пространстве. При обнаружении аномалий применяют различные методы, которые, в значительной степени отличаясь по существу, основаны на обработке данных о сетевом трафике [2, 3, 4]. В качестве сетевого трафика в задачах обнаружения сетевых аномалий рассматриваются данные о прошедшем через транзитный узел объеме информации в единицу времени. Для получения таких данных применяют зеркалирование трафика на сетевые сенсоры. Наиболее часто в качестве механизма, собирающего информацию о прошедшем через сетевой узел трафике, используют Cisco NetFlow [5].

Современные исследования позволяют утверждать [6], что значительная часть проблем, связанная с аномальной загрузкой магистральных каналов передачи данных, обусловлена аномальной активностью хостов конечных пользователей. Речь здесь может идти о работе на конечных узлах программ-участников пиринговых сетей, программ туннелирования трафика, программ-сетевых вирусов, вызывающих аномальную сетевую активность. По этой причине в указанных случаях сбор информации о трафике оправданно вести как можно ближе к конечным хостам. Сетевой сенсор может быть организован на маршрутизаторе, отделяющем сегмент локальной сети с конечными узлами от сетей более высокого ранга. В последнее время значительную долю таких маршрутизаторов составляют многофункциональные ЭВМ с операционной системой Linux. Возросший интерес к использованию подобных систем обусловлен невероятной гибкостью и широкими возможностями одновременной реализации различных сетевых ролей (сервер удаленного доступа, сервер или клиент виртуальной частной сети, маршрутизатор, телефонная станция — IP АТС и т.д.) на одном устройстве. В отмеченных случаях информация об IP трафике, собираемая с таких систем, дает полную картину сетевого поведения всех устройств в сегменте локальной сети, к которым они подключены.

Целью данной работы является исследование возможностей использования сенсора IPCAD, эмулирующего работу механизма Cisco NetFlow на маршрутизаторе в виде многофункциональной ЭВМ с операционной системой Linux, в качестве поставщика исходной информации для обработки в системах обнаружения сетевых аномалий IP трафика.

Подход к моделированию системы сбора информации о сетевом трафике

Известны случаи применения сенсора IPCAD в задачах подсчета трафика за большие периоды времени (часы, дни, месяцы) [7]. В то же время задачи обнаружения сетевых аномалий приводят к необходимости анализа детальной информации о трафике в некотором временном окне, которое у различных исследователей составляет от нескольких секунд до нескольких часов. Поскольку существует положительный опыт применения сенсора IPCAD на больших временных интервалах, представляет интерес исследование точности сенсора на малых временных интервалах — минута и менее.

С другой стороны, современные скорости каналов, обеспечивающие подключение сегментов локальных сетей к сетям более высокого ранга, например к сети Интернет, составляют единицы мегабит в секунду. И здесь представляет интерес исследование точности сенсора на скоростях от сотен килобит в секунду до десяти мегабит в секунду.

Прикладной протокол передачи данных, использующийся для тестирования, должен обладать возможностью передачи информации с заданной скоростью. Такая возможность удовлетворит потребности передачи данных на различных заданных скоростях.

Сетевая топология, применяемая дли исследования, должна включать узел-источник информации, узел-приемник информации и транзитный узел, собирающий статистику о прошедшем трафике.

С учетом приведенных соображений моделирование процесса обмена информацией проведем на скоростях передачи 100; 200; 300; 500; 800; 1300; 2100; 3400; 5500; 8900 Кбит/с. В качестве прикладного протокола будем использовать ftp – file transfer protocol (протокол передачи данных). Сетевую топологию, на которой будем проводить исследования, покажем на рис. 1. В данной топологии для моделирования трафика используется процесс передачи данных с источника данных (ftp клиент) на приемник данных (ftp сервер) через транзитный маршрутизатор. Маршрутизатор представляет собой многофункциональную ЭВМ с двумя сетевыми интерфейсами Ethernet и установленным программным сенсором IPCAD. Информация о прошедшем сетевом трафике обрабатывается на станции сбора данных. Интервалы измерения объема трафика, прошедшего через маршрутизатор, сделаем равными 60; 30; 20; 10; 6; 3 и 2 с.

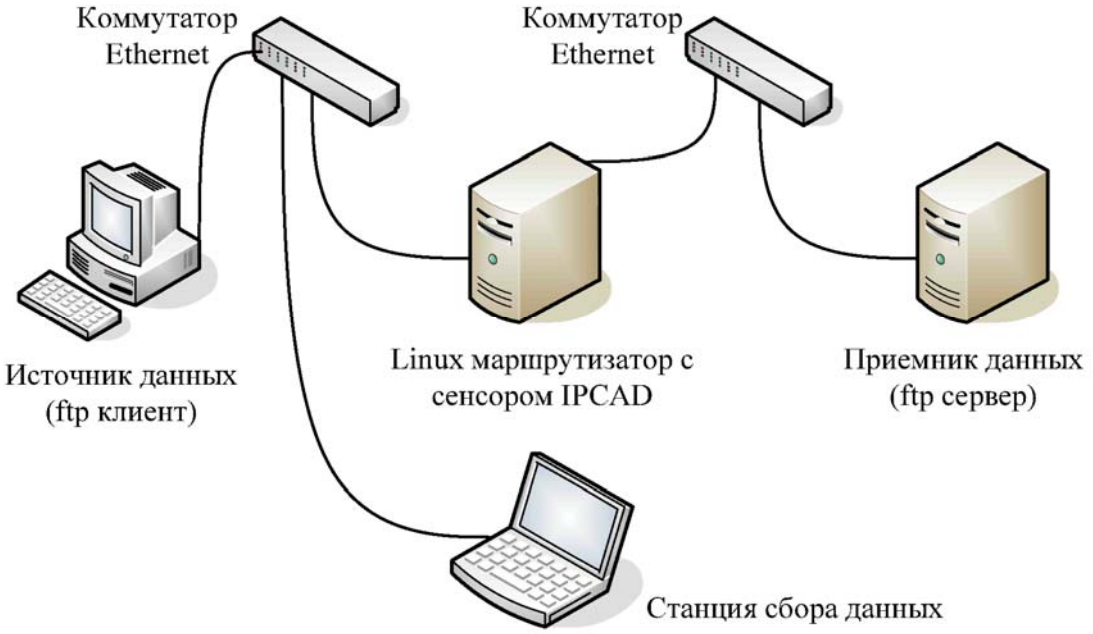


Рис.1. Сетевая топология для моделирования

Перед выбором критерия для анализа корректности работы сетевого сенсора рассмотрим некоторые конкретные кривые, иллюстрирующие результаты имитационного моделирования процесса передачи данных и сбора сетевой статистики. На рис. 2 показаны зависимости от времени объема переданной информации при передаче файла объемом 59,25 Мегабайт на выбранной сетке скоростей при интервале между соседними точками измерения количества переданной информации 10 с. Рисунок иллюстрирует тот факт, что повышение скорости передачи в некоторое количество раз снижает в то же самое количество раз время передачи. Небольшие колебания скорости передачи обусловлены спецификой транспортного протокола TCP (Transmission Control Protocol), пытающегося поднять скорость передачи информации и затем опускающего эту ско-

рость в соответствии с прикладным протоколом передачи данных ftp, зафиксировавшего эту скорость согласно требованию приложения-клиента.

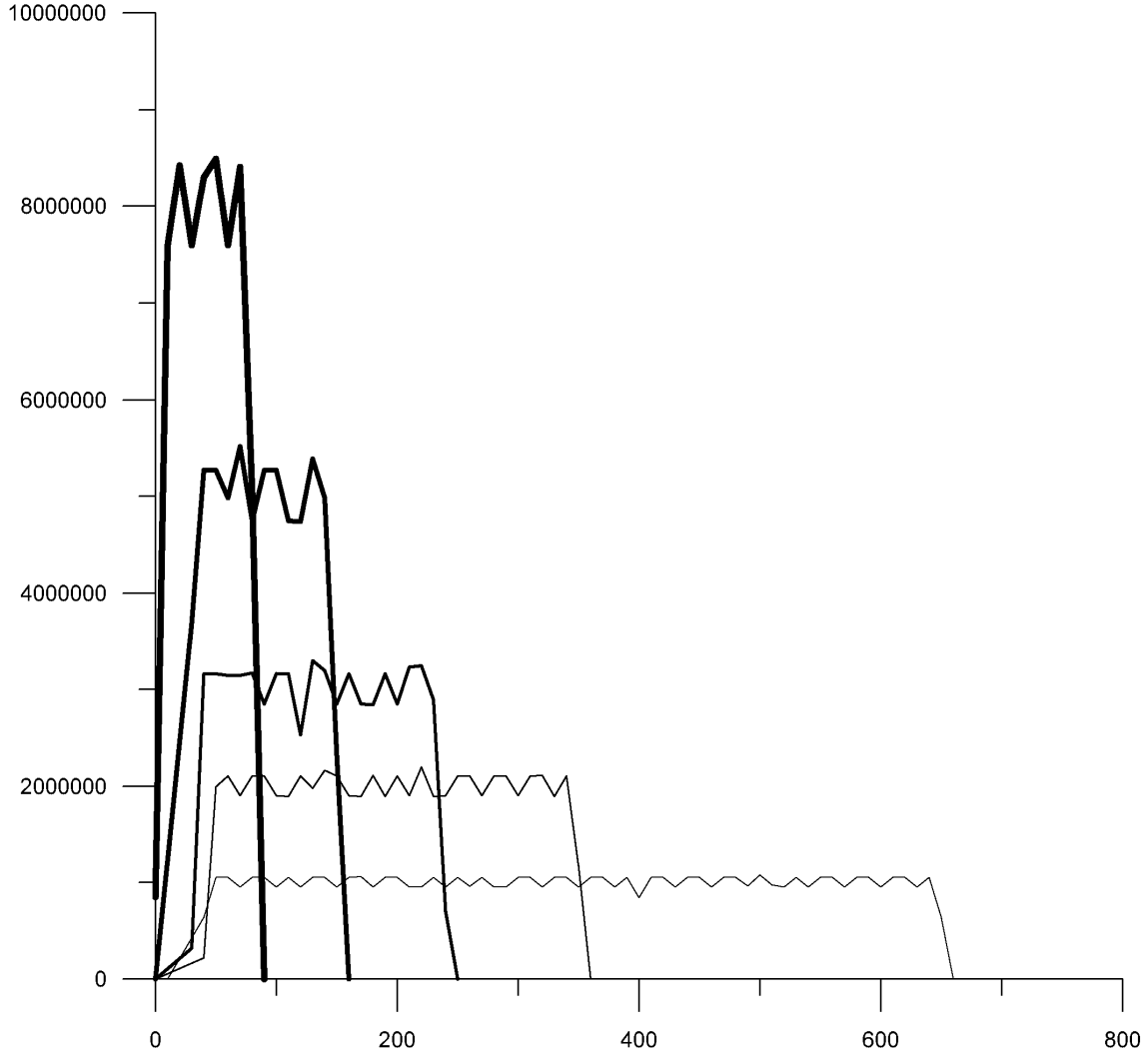


Рис. 2. Зависимости переданного объема данных от времени на различных скоростях передачи при интервале подсчета прошедшего трафика, равном 10 с

Кривые на рис. 2 будем интерпретировать как одномерные изображения. С точки зрения теории обработки изображений характеристикой сравнения некоторой оценки изображения с эталонным изображением служит нормированная среднеквадратичная ошибка ξ, вычисленная по правилу [8]:

$$\xi = \frac{\sum_{i=1}^{N}(I_i - I_i^0)^2}{\sum_{i=1}^{N}(I_i^0)^2}, \qquad (1)$$

где $i = 1..N$, N — количество точек, в которых известны изображения; $I_i, i = 1..N$ — некоторая оценка изображения; $I_i^0, i = 1..N$ — эталонное изображение. В нашем случае ситуация осложняется тем, что исходное изображение неизвестно, однако известен

объем передаваемой информации. И по этой причине в качестве интегрального показателя качества работы сетевого сенсора будем использовать величину

$$\xi = \frac{(\sum_{i=1}^{N} \hat{V}_i - V^0)^2}{\left(V^0\right)^2}, \qquad (2)$$

где $i = 1..N$, N — число точек, в которых сетевым сенсором произведены измерения; $\hat{V}_i$ — объем прошедшего трафика между i-м и $i-1$-м измерением; V^0 — известный объем передаваемой информации. Такая величина имеет смысл нормированной ошибки измерения с помощью сетевого сенсора объема передаваемой информации. Для определения качества работы сетевого сенсора исследуем зависимости ξ на выбранной сетке скоростей передачи.

Результаты моделирования показывают, что значение ξ для различных скоростей передачи не превышает 0,00055 при величине интервала измерений не менее 3 с, что соответствует ошибке измерения объема переданного трафика не более 3%. Значения ξ имеют аналогичные зависимости от скоростей передачи при различных объемах передаваемой информации. При интервале измерений 2 с и менее значение ξ резко возрастает, при этом ошибка измерения объема переданного трафика превышает 10%. Указанное явление происходит по причине пропуска сетевым сенсором значительного числа пакетов при выполнении процедуры очистки счетчика трафика через короткие интервалы времени.

Реализация имитационной модели

Для проведения моделирования реализовывалась сетевая топология, показанная на рис. 1.

Источник данных и Linux маршрутизатор реализовывались в виде виртуальных машин с помощью средства виртуализации Oracle Virtual Box 4.1.8 с операционными системами Microsoft Windows XP SP3 и Linux CentOS 6.2 в родительской операционной системе Microsoft Windows Server 2008 R2. В качестве коммутатора Ethernet между ЭВМ-источником и Linux маршрутизатором использовался виртуальный коммутатор Microsoft.

Приемник данных представлял собой отдельный ftp-сервер на базе Microsoft Windows Server 2008 R2, который подключался к Linux маршрутизатору через коммутатор Ethernet со скоростью портов 100 Мбит/с. Механизм записи данных о прошедшем трафике реализовывался в Linux системе с помощью планировщика заданий cron, при этом информация о прошедшем трафике записывалась в файлы, которые затем обрабатывались на станции сбора данных.

При максимальной скорости передачи 8900 Кбит/с загрузка процессора виртуальной машины с маршрутизатором, под который отводилось одно ядро процессора и 512 Мбайт оперативной памяти, не превышала 15%. Это позволяет утверждать, что на практике на реальных ЭВМ с числом ядер процессора не менее двух показатели качества работы сенсора будут не хуже показателей, которые наблюдались в моделируемой сетевой топологии.

Заключение

Показана возможность использования сенсора IPCAD, эмулирующего работу механизма Cisco NetFlow на маршрутизаторе в виде многофункциональной ЭВМ с операционной системой Linux, в качестве поставщика исходной информации для обработки в системах обнаружения сетевых аномалий IP трафика. Установлено, что ошибка измерения объема переданного трафика составляет не более 3 % при значении интервалов измерения от 3 с до 1 мин на скоростях передачи данных от сотен килобит в секунду до десяти мегабит в секунду.

ЛИТЕРАТУРА

1. Обнаружение закономерностей и распознавание аномальных событий в потоке данных сетевого трафика / Е. Е. Витяев [и др.]. — Вестник НГУ. Серия: Информационные технологии. — 2008. — Том 6. — Вып. 2. — С. 57—68.

2. P. Abry and D. Veitch, “Wavelet analysis of long range dependent traffic,” IEEE Transactions on Information Theory, vol. 44, no. 1, 1998.

3. P. Barford and D. Plonka, “Characteristics of network traffic flow anomalies,” in Proceedings of ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, November 2001.

4. Петров В.В. Статистический анализ сетевого трафика. — М., 2003.

5. Introduction to Cisco IOS NetFlow — A Technical Overview. — Режим доступа: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html (дата обращения 04.03.2012).

6. О влиянии трафика хостов с клиентами пиринговых сетей на загрузку магистральных каналов. Крюков, Ю. А. Исследование влияния P2P потоков на производительность магистрального канала сети «ЛАНПОЛИС» / Ю. А. Крюков, Д. В. Чернягин http://sanse.ru: сайт электронного журнала [Электронный ресурс]. — Режим доступа: http://sanse.ru/download/33 (дата обращения 04.03.2012).

7. Кузнецов А.В. Учет трафика в Linux с помощью ipcad. — Режим доступа: http://www.nixp.ru/articles/Учет-трафика-в-Linux-с-помощью-ipcad.html (дата обращения 04.03.2012).

8. Прэтт У. Цифровая обработка изображений: в 2 т: пер. с англ. — М.: Мир, 1982. — Т.1.

СВЕДЕНИЯ ОБ АВТОРАХ:

Меньших Валерий Владимирович. Начальник кафедры высшей математики. Доктор физико-математических наук, профессор.

Воронежский институт МВД России.

E-mail: menshikh@vmail.ru

Россия, 394065, проспект Патриотов, 53. Тел. (473) 227-72-87.

Телков Александр Юрьевич. Доцент кафедры электроники. Кандидат физико-математических наук, доцент.

Воронежский государственный университет.

E-mail: telkov@dpo-it.ru

Россия, 394006, Воронеж, Университетская пл., 1. Тел. (473) 220-82-84.

Menshikh Valery Vladimirovich. The chief of the chair of High Mathematics. Doctor of physical and mathematical sciences, professor.

Voronezh Instinute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 227-72-87.

Telkov Alexander Yurievich. The assistant professor of chair of Electronics. Candidate of sciences (physics and mathematics), assistant professor.

Voronezh State University.

Work address: Russia, 394065, Voronezh, Universitetskaya Sq., 1. Tel. (473) 220-82-84.

Ключевые слова: DDoS; аномалии сетевого трафика; IPcad; обнаружение аномалий.

Key words: DDoS; network traffic anomaly; IPcad; anomaly detection.

УДК 004.7.056.53

Р.А. Солодуха,
кандидат технических наук, доцент

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

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА RS-СТЕГАНОАНАЛИЗА ПРИМЕНЕНИЕМ ЕГО К ГРУППАМ ПИКСЕЛОВ РАЗЛИЧНОГО РАЗМЕРА

THE IMPROVEMENT OF THE RS-STEGANALYSIS METHOD BY APPLYING IT TO A VARIOUS PIXEL GROUP SIZE

Предлагается одно из усовершенствований метода RS-стеганоанализа графических стеганоконтейнеров. В основе лежит распространение метода на группы пикселов различного размера и получение трасологической статистики стеганографического алгоритма. Разработанная модификация метода дает более точные результаты определения размера стегановложения, особенно при атаке на базе известного стеганографического алгоритма.

The improvement of the RS-steganalysis method for graphic cover messages is offered. It is based on distribution the method to a various size group of pixels and obtaining the trace evidence statistics of the steganographic algorithm. The modification gives more accurate results for determining the steganographic content size, especially for the attack on the basis of known steganographic algorithm.

Введение

Одним из оригинальных методов статистического стеганоанализа является метод RS [1—3], впервые опубликованный в 2001 г. коллективом ученых под руководством Дж. Фридрих. Сокращение в названии расшифровывается как Regular-Singular, то есть «регулярно-сингулярный».

Суть метода состоит в следующем. Все изображение разбивается на группы по n пикселов $G(x_1,x_2,\ldots,x_n)$, где n четно, например по 2 пиксела, находящихся рядом по горизонтали. Для группы пикселов определяется функция регулярности или «гладкости» $f(G)$, в качестве такой функции можно выбрать, например, дисперсию значений внутри группы, либо просто сумму перепадов значений смежных пикселов. Под значением пиксела понимаем целое число от 0 до 255.

$$f(x_1, x_2, ...x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| .$$

Функция *F(x)* называется флиппингом и имеет свойство *F(F(x)) = x*. Определяют две функции флиппинга — F_1, соответствующую инверсии младшего бита пиксела, и F_{-1}, представляющую собой инверсию с переносом в старший бит (прибавление единицы):

$$F_1 = \begin{cases} x+1, & 0 \le x \le 254 \\ 0, & x = 255 \end{cases} \quad \text{и} \quad F_{-1} = \begin{cases} x-1, & 1 \le x \le 255 \\ 255, & x = 0 \end{cases} .$$

При применении флиппинга к группе получают преобразованную группу пикселов. Далее делят все группы пикселов на классы следующим образом:

- регулярные группы: $G \in \boldsymbol{R} \Leftrightarrow f(F(G)) > f(G)$;
- сингулярные группы: $G \in \boldsymbol{S} \Leftrightarrow f(F(G)) < f(G)$;
- неиспользуемые группы: $G \in \boldsymbol{U} \Leftrightarrow f(F(G)) = f(G)$.

В дальнейшем исследуется соотношение между группами в изображении. Определяется количество групп попавших в тот или иной класс как R_M, S_M, U_M и R_{-M}, S_{-M}, U_{-M}, где индексы M и –M означают соответственно применение F_1 и F_{-1} для получения распределения. Цель — определить, каким образом внедрение сообщения методом LSB будет влиять на вышеописанную статистику групп пикселов.

Метод основывается на статистическом предположении, что для естественного изображения, другими словами, незаполненного контейнера, характерно следующее:

$R_M \cong R_{-M}$ и $S_M \cong S_{-M}$.

Предположение основано на том, что применение F_{-1} даст то же распределение, что и F_1 на изображении, значения пикселов которого сдвинуты на единицу. Для пустого контейнера соотношение между группами не должно существенно меняться. Значительное расхождение между значениями свидетельствует о применении LSB-стеганографии. RS-стеганоанализ реагирует на естественный шум в изображениях, ограничивающий теоретически возможную точность определения длины сообщения.

Модификация метода RS-стеганоанализа

В данной статье предлагается модификация метода RS-стеганоанализа, в основе которой лежит идея распространения данного метода на группы различного размера. Анализируемым параметром является последовательность отношений регулярных групп после прямого и обратного флиппинга. В дальнейшем этот метод будем обозначать как RS-VGS (Variable Group Size).

Пусть $R_g = \dfrac{R_g^1}{R_g^{-1}}$,

где R_g^1 — количество регулярных групп после прямого флиппинга (R_M);

R_g^{-1} — количество регулярных групп после обратного флиппинга (R_{-M});

g — размер группы в пикселах, $g \ge 2$.

Заметим, что количество неиспользуемых групп для файлов 600x800 не превышает десяти при общем числе групп 240 тысяч, что с учетом соотношения R+S+U=const, позволяет отказаться от рассмотрения S-групп, ограничившись анализом R-групп.

Пусть *s* — размер вложения в процентном соотношении к размеру контейнера, тогда $R_{g,s}$ — это R_g для файла с вложением размера *s %* от максимально возможного.

Поскольку файлы формата BMP используют цветовую модель RGB, обозначим $R_{g,s}$ для канала Red, как $R_{g,s}[Red]$; для канала Blue, как $R_{g,s}[Blue]$; для канала Green,

как $R_{g,s}[Green]$. Также будем пользоваться средним значением

$$\overline{R}_{g,s} = \frac{R_{g,s}[Red] + R_{g,s}[Blue] + R_{g,s}[Green]}{3}.$$

При последовательном увеличении размера групп их количество определим по формуле

$$g_i = 2^i,\ i = 1..N;\ N = \left[log_2 \frac{W \cdot H}{100} \right],$$

где W и H — размеры изображения в пикселах по горизонтали и вертикали, символ [ ] — функция округления в меньшую сторону, получим массив значений $\overline{R}_{g,s}$.

Для совокупности изображений определим величины, тесно связанные со средним значением и дисперсией. Эти величины выбраны в связи с достаточно хорошим знанием свойств этих функций.

$$M[R_{g,s}] = \frac{1}{N} \sum_{i=1}^{N} \overline{R}_{g,s}(file_i)\ ,$$

$$\sigma[R_{g,s}] = \sqrt{\frac{1}{N} \sum_{i=1}^{N} \left[\overline{R}_{g,s}(file_i) - M[R_{g,s}] \right]^2}\ ,$$

где N — количество файлов изображений; $file_i$ — идентификатор файла.

При значениях *N, σ,* обеспечивающих репрезентативность выборки [5], значения $M[R_{g,s}]$ представляют собой статистику работы стеганографического алгоритма. В контексте криминалистической терминологии назовем это трасологической статистикой стеганографического алгоритма (программы).

Теперь атака на стеганографический контейнер с известным алгоритмом [1] сводится к получению массива значений $\overline{R}_{g,s}$ для анализируемого файла и сравнения с трасологической статистистикой.

Описание эксперимента и результаты

Метод RS-VGS был опробован на фотореалистичных изображениях, на примере стеганографических программ, реализующих методы семейства LSB: CryptArkan, StegoMagic, S-Tools, The Third Eye.

В качестве материала для исследования были выбраны фотографии с трёх различных фотоаппаратов Canon PowerShot A510, Canon DIGITAL IXUS 950 IS и Canon PowerShot S3 IS формата JPEG с разрешениями 2048×1536, 3264×2448, 2816×2112 пикселов, соответственно. При этом с каждого фотоаппарата были выбраны 3 группы фотографий: с изображением пейзажа; с изображением группы людей, с изображением одного человека.

Для подготовки стеганоконтейнеров все файлы были преобразованы в формат BPM (24-bit) с разрешением 800×600 пикселов. Проверка результатов rs-анализа пустых контейнеров с помощью критерия Манна — Уитни — Вилкоксона [6] показала однородность выборок из каждой группы, поэтому далее все группы были объединены.

Вложения было решено представить в виде архивов WinRar с максимальным сжатием, и при этом каждый файл вложения составил 10, 30, 50, 70 и 90% от ёмкости максимально возможного вложения в контейнер для выбранных программ. Сведения о размерах стегановложений и емкости контейнеров (BMP 24-bit с разрешением 800×600) для используемых программ приведены в таблице.

Сведения о размерах стегановложений и емкости контейнеров

Программа	Емкость, кБайт	Размер стегановложений, кБайт	Примечание
S-Tool	180	18, 54, 90, 126, 162	
The Third Eye	140	14, 48, 70, 98, 126	
Crypt Arkan	720	72, 216, 360, 504, 648	Используются четыре младших бита изображения
StegoMagic	179	18, 54, 90, 125, 160	

В результате эксперимента были получены зависимости математического ожидания отношения количества регулярных групп после прямого флиппинга к количеству регулярных групп после обратного флиппинга $M[R_{g,s}]$ от размера вложений (s) и количества пикселов в группе (g). На рис. 1—4 по оси абсцисс отложено количество пикселов в группе (шкала $\log_2(x)$), по оси ординат — $M[R_{g,s}]$, ($R_{g,s}$ взято в процентах), легенда показывает размер вложений в процентах от максимально возможного, например f70 — 70% вложение.

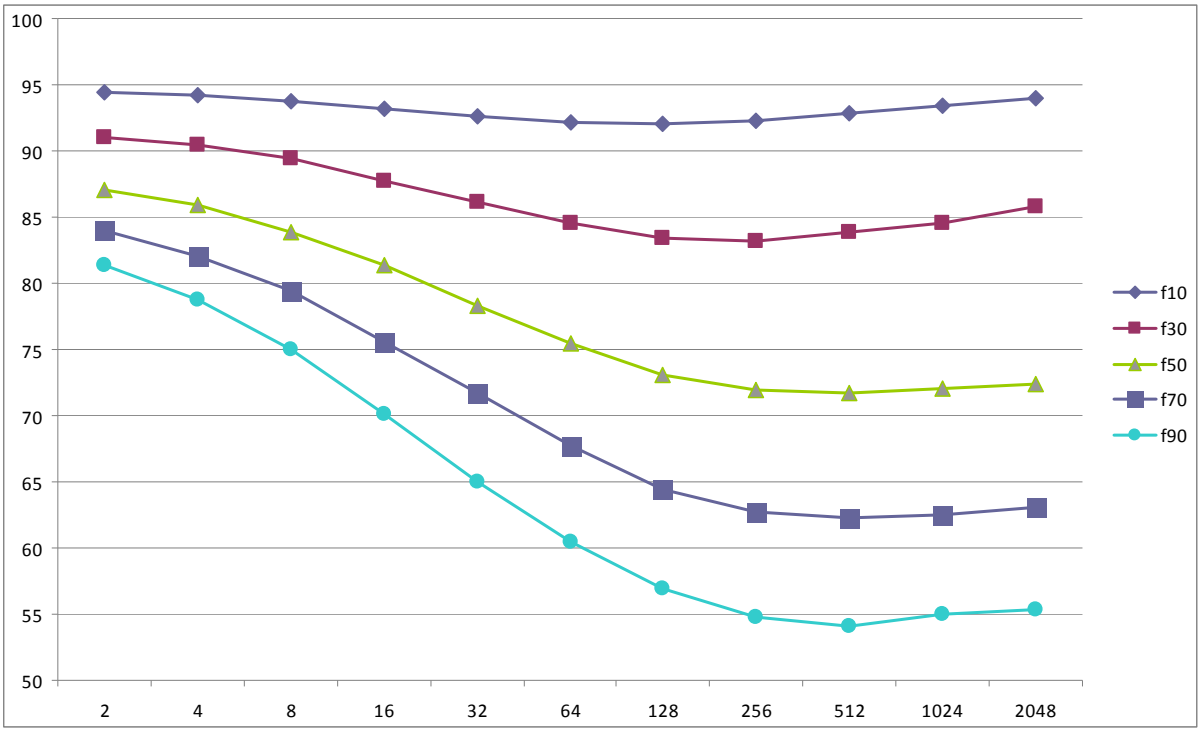


Рис. 1. Статистика работы программы CryptArkan

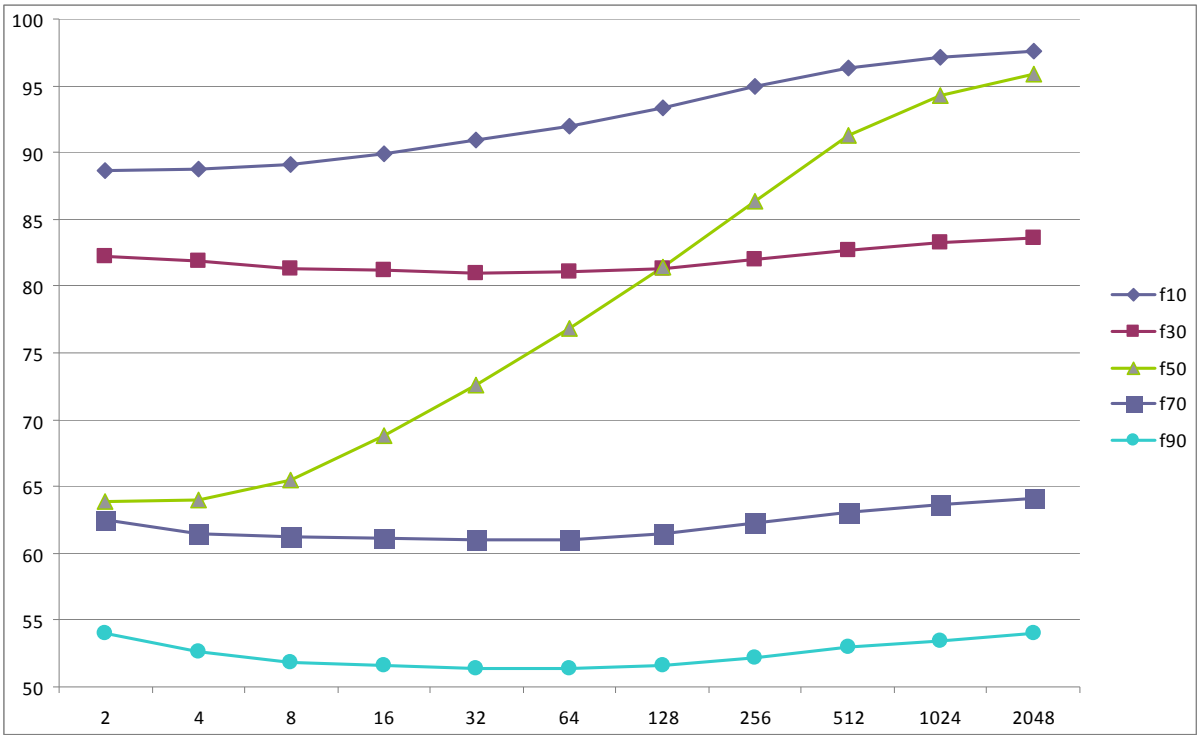


Рис. 2. Статистика работы программы StegoMagic

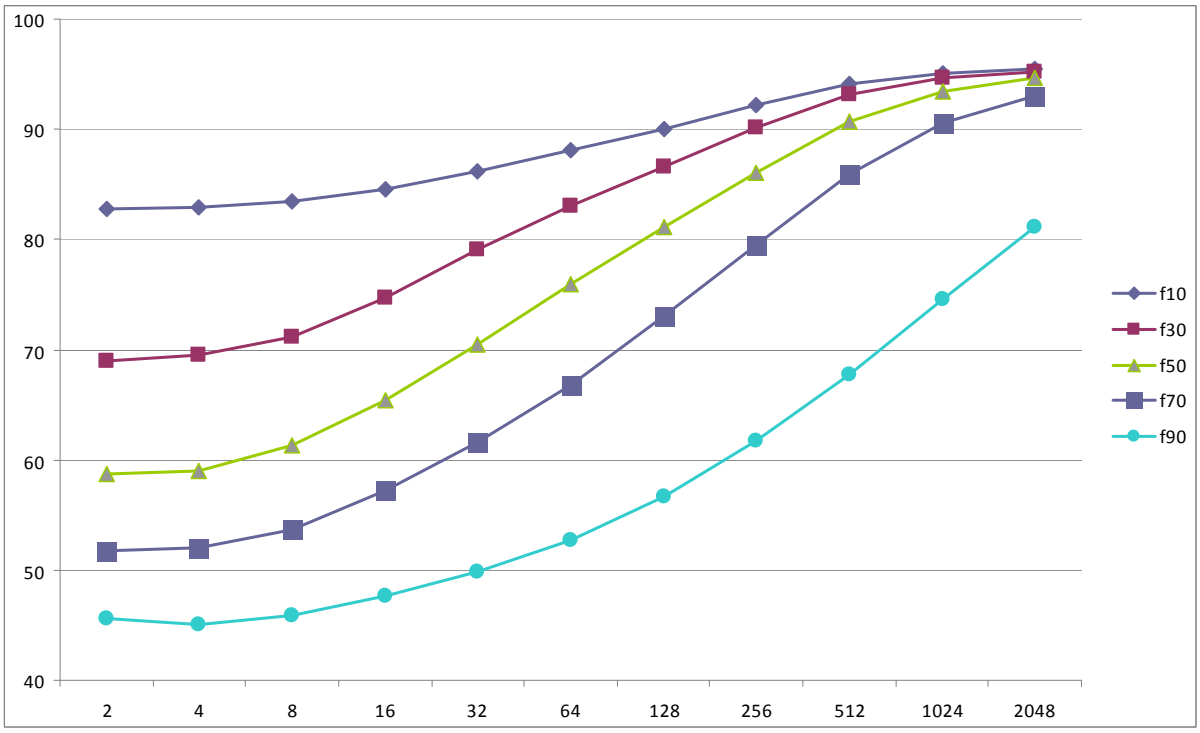


Рис. 3. Статистика работы программы S-Tool

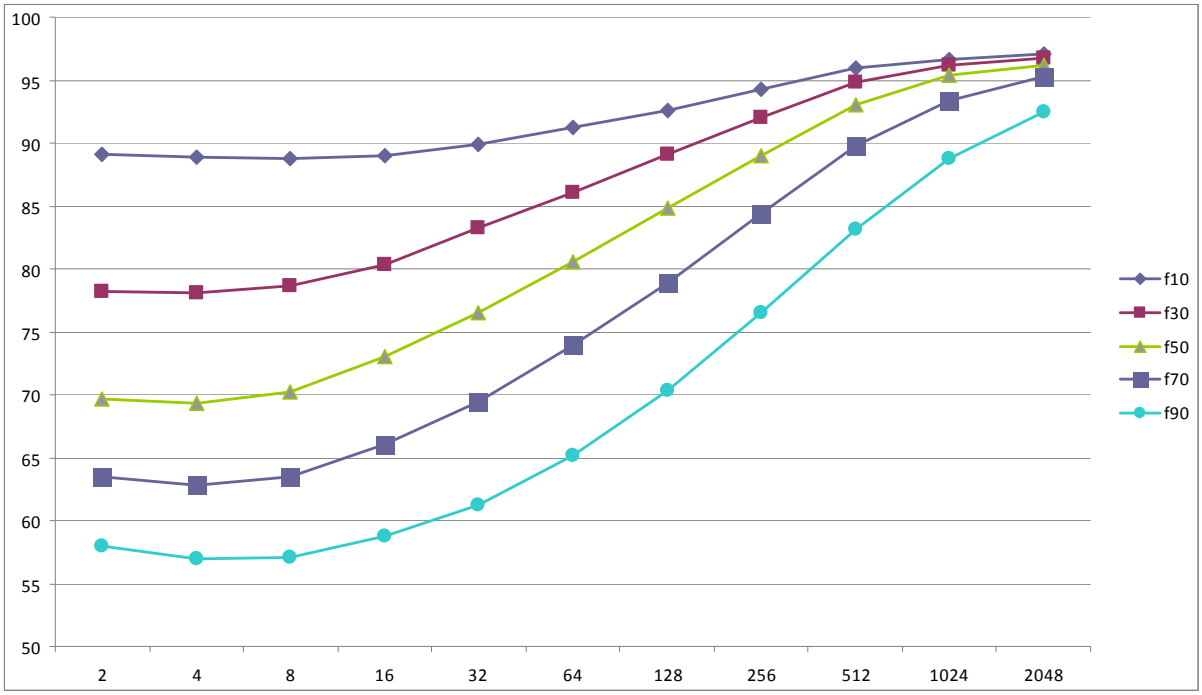


Рис. 4. Статистика работы программы The Third Eye

Анализ графиков показал, что программы S-Tool, The Third Eye и StegoMagic (при уровне вложения около 50%) используют схожие алгоритмы стегановложения, трасологическая статистика которых существенно отличается от трасологической статистики программы CryptArkan.

Заключение

Проверка разработанного метода производилась сличением кривой $\overline{R}_{g,s}$ исследуемого файла с трасологической статистикой вышеперечисленных стеганографических программ путем выбора кривой с минимальным значением среднеквадратичного отклонения от $\overline{R}_{g,s}$ исследуемого файла:

$$F_0 = \arg\min_S \left(\sum_g \left(M[R_{g,s}] - \overline{R}_{g,s} \right)^2 \right).$$

Поскольку значения трасологической статистики следуют с шагом 20%, то, в случае значительного отклонения экспериментальной кривой от статистической необходимо выбрать еще одну:

$$F_1 = \arg\min_{S \in S/\{F_0\}} \left(\sum_g \left(M[R_{g,s}] - \overline{R}_{g,s} \right)^2 \right),$$

тогда результат будет находиться в интервале (F_0, F_1).

Таким образом, RS-VGS не только обнаруживает наличие вложений, но более точно (погрешность не более 25% от размера вложения), чем RS, определяет их размер и предполагаемую программу, с помощью которой производилось вложение. Таким образом, RS-VGS является адаптацией метода RS-стеганоанализа к задаче стеганоанализа изображений на основании известного стеганоалгоритма и расширяет возможности стеганоаналитической экспертизы [4].

ЛИТЕРАТУРА

1. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский [и др.]. — М.: Вузовская книга, 2009. — 220 с.

2. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images, ICME 2000, New York City, July 31—August 2, New York.

3. J. Friedrich, G. Miroslav, R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghampton, New York: SUNY, 2001.

4. Солодуха Р.А. Стеганоанализ как подвид информационно-компьютерной экспертизы // Обеспечение общественной безопасности в ЦФО РФ: сб. материалов Международной научно-практической конференции. — Воронеж: Воронежский институт МВД России, 2007. — Ч.4. — С.221—223.

5. Копылов А.Н., Солодуха Р.А., Перминов Г.В. Определение объема репрезентативной выборки в целях получения трасологической статистики стеганографических программ // Охрана, безопасность, связь — 2011: материалы Международной научно-практической конференции. — Воронеж: Воронежский институт МВД России, 2012. — Ч.2. — С.138—140.

6. Кобзарь А.И. Прикладная математическая статистика. Для инженеров и научных работников. — М.: Физматлит, 2006. — 816 с.

СВЕДЕНИЯ ОБ АВТОРАХ:

Солодуха Роман Александрович. Доцент кафедры автоматизированных информационных систем ОВД. Кандидат технических наук, доцент.
Воронежский институт МВД России.
E-mail: aisovd@vimvd.ru
394065, г.Воронеж, проспект Патриотов, 53. Тел. (473) 2476-477.

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.

Solodukha Roman Alexandrovich. Assistant professor of the automated information systems of Law Enforcement Agencies chair. Candidate of sciences (technical), assistant professor.
Voronezh Institute of the Ministry of Interior of Russia.
Work address: 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2476-477.

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: стеганоанализ; метод наименьших значащих бит; атака на основании известного алгоритма; rs-метод, bmp-файл.

Key words: steganalysis; least significant bits method (LSB); the attack on the basis of well-known algorithm; rs-method; bmp-file.

УДК 519.68

О.В. Багринцева

С.В. Белокуров,
доктор технических наук, доцент,
Воронежский институт ФСИН России

УПРАВЛЕНИЕ КАЧЕСТВОМ ПРИНИМАЕМЫХ РЕШЕНИЙ ПРИ МОДЕЛИРОВАНИИ СИСТЕМЫ ОХРАНЫ ОБЪЕКТОВ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ

QUALITY MANAGEMENT OF ACCEPTED DECISIONS AT MODELLING SYSTEM OF PROTECTION OF OBJECTS IN CONDITIONS OF DELIBERATE BARRIERS

Рассматривается проблематика моделирования системы охраны пространственно-удаленных объектов с целью повышения эффективности принятия управленческих решений по обеспечению их защищенности.

The problematics of modelling of system of protection of the spatially-removed objects with objective of increase of efficiency of acceptance of administrative decisions on maintenance of their security is considered.

Степень воздействия на моделируемую систему охраны преднамеренных помех определяется в основном двумя факторами: техническим обеспечением средств постановки преднамеренных помех и уровнем квалификации нарушителя [1].

С этой целью необходимо провести анализ поведения нарушителя при проникновении на охраняемый объект с учетом уровня профессиональной подготовки нарушителя. Наличие более полной информации о профессиональном состоянии нарушителя позволяет точнее разработать план технической защиты объекта от проникновения. Сбор такого рода информации является достаточно трудным и, как правило, базируется на статистических данных по правонарушениям в данном регионе. Однако статистические данные содержат информацию об уже совершенных преступлениях и не позволяют обозначить перспективы развития техники проникновения и уровень профессиональной подготовки нарушителя. В этом случае необходимо провести анализ технического уровня развития средств взлома (обхода) препятствий, входящих в систему охраны объекта.

Как уже было отмечено ранее [2, 3], с целью преодоления системы защиты объекта, содержащей средства контроля среды распространения до охраняемой территории (объекта), могут применяться средства создания активных (пассивных) преднамеренных помех. Аппаратурная реализация указанных видов помех по подавлению объемных извещателей возможна как специально разработанными средствами создания помех, основу которых составляют малогабаритные передатчики помех, предназначенные для защиты от обнаружения нарушителя, так и средствами постановки пассивных помех.

Выбор того или иного средства создания помех по противодействию техническим средствам охранной сигнализации (ТС ОС) осуществляется на основании их тактико-технических характеристик, способов применения, ожидаемого эффекта воздействия на приемные устройства извещателей охраны.

На основании анализа материалов, посвященных вопросам применения средств создания помех [1—5], можно предположить следующий алгоритм их применения при вскрытии пространственно-удаленных объектов.

Заблаговременно, до начала проникновения на охраняемый объект, нарушитель размещает средство постановки пассивных помех на участке радиотрассы «центр управления (ПЦО — пульт централизованной охраны) — предполагаемый к вскрытию объект». Например, на участке радиотрассы распространяются металлизированные пластинки, размер которых выбирается с учетом несущей частоты рабочего сигнала подавляемого средства.

Тем самым достигается эффект ослабления зондирующего сигнала, что в итоге приводит к выравниванию мощностей полезного (зондирующего) уже ослабленного сигнала в радиоканале и уровнем непреднамеренных шумов, излучаемых радиоэлектронными средства другого целевого назначения по побочным каналам излучения, находящиеся в данном районе.

На приемной стороне (в приемном устройстве ПЦО) полезный сигнал не выделяется из шумов, что приводит к пропуску сигнала тревоги. Как следствие, реакция на поступивший вызов отсутствует и происходит несанкционированное вскрытие пространственно-удаленного объекта.

Данная задача является частным случаем задачи оптимального синтеза системы контроля [1—3], когда тактико-технические характеристики отдельных средств заданы априорно, и может быть сформулирована следующим образом:

Определить оптимальное радионаправление передачи информации в системе охраны пространственно-удаленных объектов, построенной на основе средств радиосвязи.

В качестве показателя эффективности функционирования централизованной системы охраны, в отличие от предложенного ранее [2, 3, 5], выберем величину совокупных затрат на организацию деятельности подразделения охраны за отчетный период.

Математическая постановка данной задачи имеет вид:

$$J = \arg\min_{\{\tilde{W} \in W\}} \Pi\left(\lambda, \mu, K_{кс}\right), \qquad (1)$$

$$t \le t_{прон}\ ; Y^0 \le Y_{\max}\ ;\ E^0 \ge E_{\min}\ ;\ L^0 \le L\ ;$$

$$\lambda = f\left(t_{прон}, t_{крим}\right);\ \mu = f\left(M, T^0\right);\ K_{кс} = f\left(P_{пер}, L^o, E_L\right)$$

$$W = \{W_n\}\ ; W_n = f\left(P_{рот\_n}, Y^0\right);\ T^0 = \min\{t_{mk}\};\ L^0 = \left\{L_n^0\right\};$$

$$L_n^0 = F\left(Y_n^0, R_{opt}\right);\ Y^0 = \left\{Y_n^0\right\};\ E^0 = \left\{E_n^0\right\},$$

где $\Pi\left(\lambda, \mu, K_{кс}\right)$ — финансовые затраты подразделений охраны за отчетный период; W — множество вариантов постановки помех при проникновении нарушителя на охра-

няемый объект; T^0 — минимально допустимое время реагирования системы охраны на вызов с охраняемого объекта; t_{mk} — действительное время прибытия m-й группы задержания на k-й охраняемый объект; Y^0 — множество оптимальных значений мощности излучения ретрансляторов, находящихся в зоне ответственности ПЦО; Y_n^0 — оптимальная излучаемая мощность n-го ТС ОС, ограниченная параметром Y_{max}; E^0 — надежность моделируемой системы охраны; M — количество ГЗ в зоне ответственности подразделения охраны; $K_{кс}$ — качество канала связи передачи информации тревожного извещения; λ — интенсивность поступления сигналов тревожного извещения на ПЦО; μ — интенсивность реакции личного состава вневедомственной охраны на поступающие вызовы; E_L — надежность l-го ретранслятора; $P_{пер}$ — вероятность передачи информации по каналу связи; L — количество ретрансляторов в зоне ответственности подразделения охраны; L^0 — минимально необходимое количество задействованных для передачи информации тревожного извещения ретрансляторов, находящихся в зоне ответственности ПЦО; E_n^0 — надежность моделируемого направления передачи сигнала тревожного извещения; R_{opt} — оптимальная дальность передачи информации от охраняемого объекта на ПЦО; $F\left(Y_n^0, R_n^0\right)$ — функционал от перечисленных функций; k— количество охраняемых объектов в зоне ответственности подразделения охраны; U — количество ТС ОС на k-м охраняемом объекте.

Величина $П\left(\lambda, \mu, K_{кс}\right)$ определяется по формуле:

$$П\left(\lambda, \mu, K_{кс}\right) = П_{охрана} + П_{текущ} + П_{потери}\left(\lambda, \mu, K_{кс}\right). \quad (2)$$

Применительно к расходам на организацию технической охраны объектов собственности, затрачиваемую непосредственно ВО, величина $П_{охрана}$ определяется как сумма затрат, выделяемых на монтаж, техническое обслуживание, эксплуатационные расходы содержания ретрансляторов и определяется по формуле:

$$П_{охрана} = \sum_{z=1}^{Z} П_l + \sum_{z=1}^{Z} П_{монт\_z} + \sum_{z=1}^{Z} П_{эксп\_z}, \quad (3)$$

где $П_z$ — стоимость z-го ретранслятора; $П_{монт\_z}$ — стоимость монтажа z-го ретранслятора; $П_{эксп\_z}$ — стоимость эксплуатации технического средства в течение года, определяется в соответствии с [2].

Величина $\sum_{z=1}^{Z} П_{монт\_z}$ определяется исходя из первого раздела «Сметного расчета на производство работ по оборудованию объекта системой охраны», приведенные к одному году эксплуатации из расчета десятилетнего срока службы [3].

Здесь необходимо отметить, что установка и техническое обслуживание средств охраны на каждом объекте собственности осуществляется непосредственно за счет заказчика и, соответственно, не является статьей расхода подразделений вневедомственной охраны.

Величина $П_{текущ}$ определяется как сумма затрат, необходимых для обеспечения деятельности М групп задержания $П_{тек\_m}$:

$$П_{текущ} = \sum_{m}^{M} П_{тек\_m} . \quad (4)$$

Необходимо отметить, что как расходы заказчика по организации охраны на объекте собственности, так и сокращение затрат на содержание личного состава подразделений охраны, в работе не исследовались и принимались равной постоянной величине, усредненной на основании опыта охраны аналогичных объектов собственности.

Величина материальных затрат обслуживания охраняемых объектов $П_{потери}(\lambda, \mu, К_{кс})$, охрана которых осуществляется дистанционно посредством передачи контрольных (тестовых) сигналов по радиоканалу, оценивается на основании классификационной модели каждого объекта, основу которой составляет ранговая характеристика степени их важности и зависит от нанесенного собственнику объекта ущерба, вызванного кражей с охраняемого объекта, и определяется по формуле:

$$П_{потери}(\lambda, \mu, К_{кс}) = П_{страх}\Big|_{\substack{\lambda>\mu \\ К_{кс}\le К_{треб}}} . \quad (5)$$

Как показывает проведенный анализ [2—4], сокращение размера выплачиваемого ущерба зависит от: уменьшения интенсивности поступления вызовов с охраняемых объектов — λ; увеличения интенсивности устранения вызовов группами задержания — μ; за счет достижения требуемого качества передачи информации тревожного извещения $К_{кс}$.

Интенсивность поступления вызовов с охраняемых объектов характеризуется криминогенной обстановкой в зоне ответственности ПЦО и зависит от количества ложных вызовов с охраняемого объекта, обусловленными техническими проблемами, возникающими при эксплуатации извещателей охраны (ошибки при установке, влияние возмущающих воздействий, несвоевременность технического обслуживания и т.д.).

Увеличение интенсивности выявления нарушений, наряду с организационными мероприятиями (увеличение количества экипажей ГЗ, повышение уровня профессиональной подготовки личного состава подразделений вневедомственной охраны), зависит также и от сокращения общего времени реакции системы охраны на возмущающие воздействие.

Данное сокращение, в первую очередь, становится возможным при сокращении времени прибытия групп задержания на охраняемый объект t_{mk}, что достигается за счет их оптимального расположения в пределах зоны ответственности ПЦО [2, 3].

Анализ задачи (1) позволяет провести ее декомпозицию на ряд самостоятельных подзадач, где в качестве основной, ранее не решаемой задачи, является задача поиска оптимального маршрута передачи информации с применением ретрансляторов, размещенных в пределах зоны ответственности вневедомственной охраны.

Решение первой задачи заключается в определении маршрута передачи информации, рационального количества задействованных ретрансляторов, выборе оптимальных параметров функционирования ретрансляторов, при которых обеспечивается достижение минимума финансовых потерь. Решение задачи осуществляется применительно к конкретным типовым условиям, учитывающим как радиоэлектронную обстановку, так и количество, расположение, охраняемых объектов.

В качестве второй задачи выбрана задача оптимизации параметров сигналов, циркулирующих в контуре управления сложной пространственно-удаленной системой охраны.

Решение задачи оптимизации расходов подразделения охраны позволяет оценить эффективность функционирования ретрансляторов в условиях временных, пространственных и энергетических ограничений.

ЛИТЕРАТУРА

1. Основы информационной безопасности: учебник для высших учебных заведений МВД России / под ред. В.А. Минаева и С.В. Скрыля. — Воронеж: Воронежский институт МВД России, 2001. — 464 с.

2. Методы и средства автоматизированного управления подсистемой контроля целостности в системах защиты информации: монография / Е.А. Рогозин [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2003. — 165 с.

3. Сумин В.И., Немченко А.Ю., Орлов Д.О. Пути повышения безопасности охраны пространственно-распределенных объектов от проникновения нарушителя: монография. — Воронеж: Воронеж. гос. техн. ун-т, 2003. — 110 с.

4. Душкин А.В. Методическое обеспечение системы выявления несанкционированных воздействий на информационные телекоммуникационные системы специального назначения в условиях ограничения временного ресурса: монография. — Воронеж: ВАИУ, 2010. — 192 с.

5. Белокуров С.В., Багринцева О.В. Особенности функционирования системы контроля и управления доступом в интегрированных системах безопасности // Проблемы обеспечения надежности и качества приборов, устройств и систем: межвуз. сб. науч. тр. — Воронеж: Воронеж. гос. техн. ун-т, 2011. — С. 60—63.

СВЕДЕНИЯ ОБ АВТОРАХ:

Багринцева Оксана Владимировна. Адъюнкт кафедры автоматизированных информационных систем ОВД.

Воронежский институт МВД России.

E-mail: ganych-oksana@rambler.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. 8(473)279-32-33.

Белокуров Сергей Владимирович. Профессор кафедры управления и информационно-технического обеспечения. Доктор технических наук, доцент.

Воронежский институт ФСИН России.

E-mail: bsvlabs@mail.ru

Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. 8(473) 260-68-19.

Bagrintseva Oksana Vladimirovna. Post-graduate cadet of the chair of Automated Information Systems of the Law Enforcement Agencies.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8(473) 279-32-33.

Belokurov Sergey Vladimirovich. Professor of chair of Management and Information and Technical Providing. Doctor of sciences (technical), assistant professor.

Voronezh Institute of the Federal Service of Execution Punishment of Russia.

Work address: Russia, 394072, Voronezh, Irkutskaya, 1a. Tel. 8(473) 260-68-19.

Ключевые слова: моделирование систем охраны; принятие управленческих решений; преднамеренные помехи.

Key words: modelling of systems of protection; adoption of administrative decisions; premeditated noises.

УДК 681.3

С.К. Горлов,
кандидат технических наук, доцент

В.А. Родин,
доктор физико-математических наук, профессор

ОСОБЕННОСТИ ЛОГНОРМАЛЬНОГО РАСПРЕДЕЛЕНИЯ И ПРОГРЕССИВНАЯ ШКАЛА ПОДОХОДНОГО НАЛОГА В РОССИИ

FEATURES OF LOGNORMAL DISTRIBUTION AND ASCENDING SCALE OF SURTAX IN RUSSIA

Построена модель прогрессивной шкалы подоходного налога, учитывающая современные статистические данные по распределению доходов населения районов России. С помощью компьютерной программы проведен анализ целесообразности введения прогрессивного налогообложения.

The model of an ascending scale of the surtax, considering modern statistical data on distribution of incomes of the population of areas of Russia is constructed. By means of the computer program the analysis of expediency of introduction of the progressive taxation is carried out.

Введение

Одним из ведущих положений балансировки финансовой структуры в обществе выступает социальная направленность схем и методов налогообложения во всем мире. Так, президент США выступил в 2011 году с предложением довести высший процент прогрессивного подоходного налога США до 30-35%. Многие развитые страны Европы (Дания, Швеция и др.) давно и успешно используют прогрессивную шкалу налогов на доходы населения. В настоящее время в России происходит стихийное введение «дифференцированного подхода» в «побочное», косвенное налогообложение. Так произошло с системой дорожных штрафов в разных регионах страны, есть проект введения «налога на роскошь». В основе этих новых реформ лежит принцип, по мнению авторов, абсолютно правильный, когда более богатые слои общества платят больше, чем бедные. В НК РФ отмечено, что положение по введению и исполнению налогов должно

сглаживать финансовые неравенства разных слоев населения. При равномерном подоходном налоге в 13% это положение остается пустым заклинанием.

Опираясь на современные статистические исследования, мы привели определенную модель прогрессивного налогообложения. С помощью компьютерной программы исследуется численная зависимость всей суммы сбора налога по данной шкале от параметров распределения легальных доходов населения в различных районах России. Аналитически вычислена относительная предельная возможность логнормального распределения. Данные можно использовать для косвенного определения возможных нетрудовых доходов отдельных физических лиц.

Определение налоговой шкалы

Пусть $T = (t_0; a_1, t_1; ...; a_k, t_k)$ — упорядоченный набор $2k+1$ чисел. Числа $a_1, ...a_k$ строго возрастают и называются делениями шкалы. Числа $t_0, t_1, ..., t_k$ из промежутка [0,1) называются налоговыми ставками. Величина налога определяется по по формуле:

$$N(x) = \begin{cases} t_0 x, & 0 \le x \le a_1 \\ t_1 x, & a_1 < x \le a_2 \\ & \dots \\ t_k x, & x > a_k \end{cases} \qquad (1)$$

Налоговая шкала называется прогрессивной, если налоговые ставки строго возрастают.

Функция распределения легальных доходов населения

Известно [1], что легальный доход в расчёте на одного налогоплательщика представляет собой случайную величину X, принимающую значения $x \in [0,+\infty)$ и распределённую по логнормальному закону с плотностью распределения $f(x) = \frac{1}{\sigma\sqrt{2\pi}} \frac{1}{x} \exp\left\{ -\frac{(\ln x - \mu)^2}{2\sigma^2} \right\}$, где $\sigma \ge 0$. В отличие от нормального закона, математическое ожидание и дисперсия случайной величины X для данного логнормального закона взаимозависимы. Формулы для их определения имеют вид:

$$\mu^* = M(X) = e^{\mu + \sigma^2/2}, \; s = (\sigma^*)^2 = D(X) = \left(e^{\sigma^2} - 1\right) e^{2\mu + \sigma^2}. \qquad (2)$$

Эти формулы имеют два параметра, которые связаны с нормальным распределением и статистическими данными. Современные статистические данные мы используем из работы [2]. Несмотря на то что логнормальное распределение непосредственно связано с нормальным распределением, оно имеет одно важное качество, существенно влияющее на результаты моделирования в нашей работе, а именно аналитическую зависимость между математическим ожиданием и дисперсией.

Пусть N — количество налогоплательщиков, $t(x)$ — ставка подоходного налога, зависящая от величины дохода. Тогда совокупный налог, собранный со всех налогоплательщиков, равен $S = N \int_0^\infty t(x) x f(x) dx$. Если $t(x) = const$, то получим равномерную шкалу налогообложения: $S = N \int_0^\infty const\, x f(x) dx = const N \mu^*$. В настоящее время в России ставка равна 13%, поэтому $S_R = 0.13\, N\, \mu^*$.

Ниже мы приводим алгоритм интерактивной компьютерной программы, позволяющей, сравнивая с указанным совокупным налогом S_R, численно оценить эффективность введения построенной прогрессивной модели налогообложения доходов физических лиц, задавая параметры распределения μ, σ.

В работе показано, что, освободив полностью от налога малоимущий слой населения с помощью прогрессивной шкалы, можно не только сохранить прежний уровень сбора суммы налога S_R, но и увеличить его.

Оценка степени неравенства распределения доходов населения

Степень неравенства доходов оценивают коэффициентом Джини (Рейнбоу). Известна зависимость степени неравенства доходов населения и количества корыстных видов преступлений. Точнее, в работе [2] получен положительный коэффициент корреляции между коэффициентом Джини и коэффициентом корыстных видов преступности. Большое значение коэффициента Джини показывает неблагоприятное состояние социального климата и необходимость перераспределения доходов, возможно с помощью введения прогрессивной шкалы налога на доходы физических лиц. На основе статистических данных работ [1,2] вычисляем коэффициент Джини для различных районов России. Пусть $F(x)$ — интегральная функция распределения дохода в обществе. Решим уравнение $F(x) = 0{,}9$, т.е. найдем величину такого дохода $x^* = x(0{,}9)$, не менее которого имеют 10% самых высокодоходных членов общества; затем решим уравнение $F(x) = 0{,}1$, т.е. найдем величину дохода $x_* = x(0{,}1)$, менее которого имеют 10% членов общества с самыми низкими доходами. Отношение $Dn = \dfrac{x^*}{x_*}$ называется **коэффициентом Джини**. В благополучных Норвегии, Дании, Швеции этот коэффициент не превышает **6**, в нашей стране и в некоторых других коэффициент значительно выше, что говорит о социальном неблагополучии.

Вычислим коэффициент для логнормального распределения при различных параметрах распределения. Уравнение $F(x^*) = 0.9$ для логнормального распределения имеет вид:

$$\frac{1}{\sqrt{2\pi}\,\sigma}\int_0^{x^*}\frac{1}{u}\exp\left[-\frac{(\ln u-\mu)^2}{2\sigma^2}\right]du = 0.9\,.$$

Заменой переменной $t = \dfrac{\ln u \big/ \exp\mu}{\sigma}$ его можно свести к уравнению:

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{(\ln x^*-\mu)\big/\sigma}\exp\left[-\frac{t^2}{2}\right]dt = 0.9\,,$$

а для случая $\ln x^* > \mu$ получаем уравнение, содержащее интегральную функцию Лапласа,

$$\frac{1}{2} + \Phi\left[\frac{\ln x^* - \mu}{\sigma}\right] = 0.9\,.$$

По таблице находим решение $\ln x^* \big/ \exp\mu \approx \sigma \times 1.28$.

Аналогично для нижнего уровня состояния x_* имеем равенство:

$$\frac{1}{\sqrt{2\pi}\ \sigma}\int_0^{x_*}\frac{1}{u}\exp\left[-\frac{(\ln u-\mu)}{2\sigma^2}\right]du=0.1,$$

так как $\ln x_* < \mu$, то в силу симметрии кривой Гаусса, решение уравнения

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{(\ln x^*-\mu)/\sigma}\exp\left[-\frac{t^2}{2}\right]dt=0.1$$ имеет знак минус, $\ln x_*/\exp\mu\approx-\sigma\times1.28$.

Определяя отношение $Dn=\frac{x^*}{x_*}$, замечаем, что значение коэффициента не зависит от параметра μ, который характеризует средний легальный доход. Важным и главным является параметр σ, который и характеризует разброс.

Мы располагаем усредненными данными параметра σ по разным районам России только за 1998 год. Средняя дисперсия распределения легальных доходов России [1]: $\sigma(1998)=1.12$.

Получаем $Rn=\frac{x^*}{x_*}=\exp(\sigma\times2.56)\approx17.6.$ Для Москвы значение дисперсии еще выше, в настоящее время оно оценивается как величина, больше 1.5.

И коэффициент Джини для Москвы

$$Rn(Москва)=\frac{x^*}{x_*}=\exp(\sigma\times2.56)>46.$$

Сложившееся в настоящее время в России серьезное различие в уровне благосостояния разных слоев населения недопустимо. Значение коэффициента Рейнбоу, превышающее 10 единиц, в основных развитых странах считается сигналом к возможным забастовкам и даже революционным действиям. Одним из принятых способов сгладить уровень благосостояния является введение прогрессивной шкалы налогообложения.

Описание примера прогрессивной шкалы

В формуле (1) с бедных людей, доход которых не превышает некоторого значения a_1, налог вообще не берётся $t_0=0$ (социальная направленность налоговой политики). Также примем $t_{n+1}=0$, т.е. со сверхбогатых людей налог в общепринятом смысле тоже не берётся, поскольку, во-первых, вероятность иметь очень высокий доход пренебрежимо мала (смотри ниже), а, во-вторых, по отношению к этим людям проводится особая политика помощи государству.

Тогда формула сбора прогрессивного налога имеет вид:

$$S=N\mu^*\sum_{k=1}^{n}t_k\left[\Phi\left(\frac{\ln a_{k+1}-\mu-\sigma^2}{\sigma}\right)-\Phi\left(\frac{\ln a_k-\mu-\sigma^2}{\sigma}\right)\right],$$

где $\Phi(x)=\frac{1}{\sqrt{2\pi}}\int_0^x e^{-x^2/2}dx$ — функция Лапласа.

Предложим следующую схему налогообложения:

$$t(x) = \begin{cases} 0.13, & 0.2\mu^* \le x < 5\mu^* \\ 0.15, & 5\mu^* \le x < 10\mu^* \\ 0.20, & 10\mu^* \le x < 20\mu^* \\ 0.30, & 20\mu^* \le x < 50\mu^* \\ 0.45, & 50\mu^* \le x < 90\mu^* \end{cases} ..$$

Блок-схема алгоритма программы расчета налогов приведена на рис. 1.

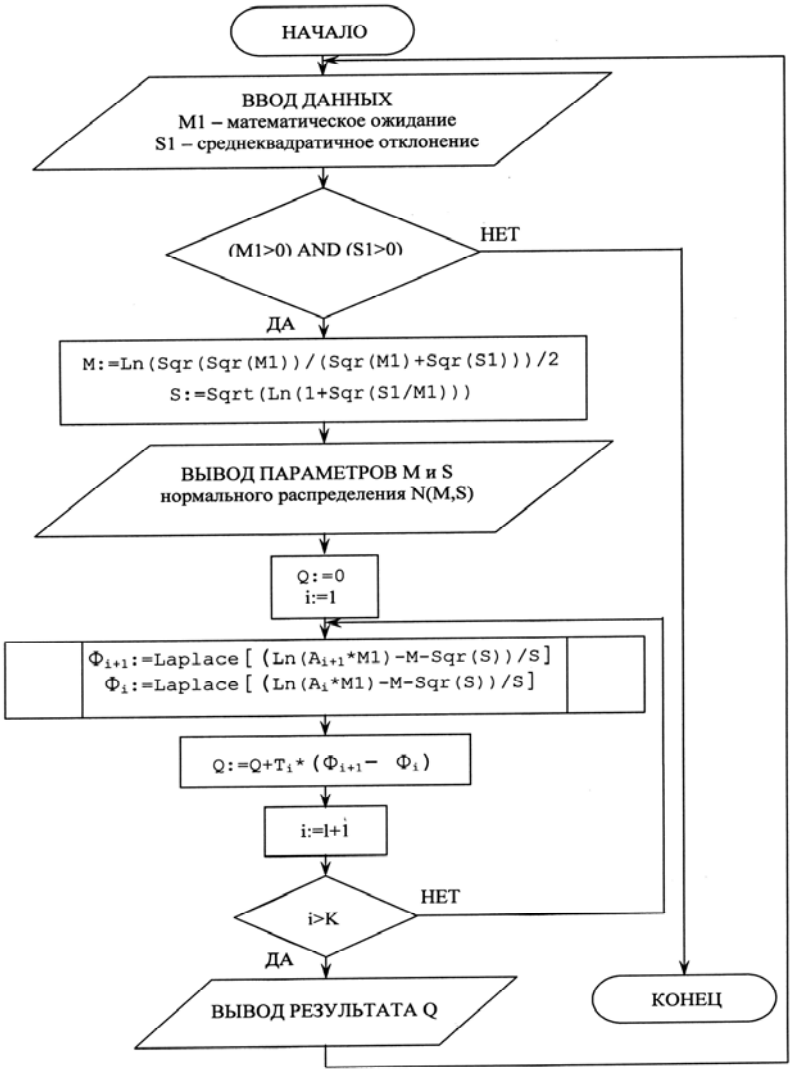


Рис.1. Блок-схема алгоритма программы расчета налогов

Расчет прогрессивного подоходного налога с помощью программы

Предполагаем, что доходы X населения распределены по логнормальному закону. Числовые характеристики данного распределения: μ^* — математическое ожидание (средний доход тыс. руб.), s^* — среднеквадратичное отклонение (разброс доходов, тыс. руб.), μ^* и s^* выражаются через параметры μ и σ нормального распределения. Используется следующая шкала разбиения доходов:

$$(0.2\,\mu^*, 5\,\mu^*), (5\,\mu^*, 10\,\mu^*), (10\,\mu^*, 20\,\mu^*), (20\,\mu^*, 50\,\mu^*), (50\,\mu^*, 90\,\mu^*).$$

Процентные ставки налога соответственно равны 13%, 15%, 20%, 30%, 45%.

При $x \le 0.2\mu^*$ налог не взимается из соображений социальной справедливости. С очень больших доходов $x > 90\mu^*$ (эта граница будет аналитически обоснована) налог не взимается в общепринятом смысле. Предполагается, что со сверхбогатыми людьми проводится особая политика помощи государству.

Таблица численного анализа свойств прогрессивной шкалы

	$\mu^* = 15$	$\mu^* = 15$	$\mu^* = 20$	$\mu^* = 20$
s^*	Q	σ	Q	σ
20	0.133	1.011	0.131	0.833
40	0.151	1.447	0.142	1.269
60	0.162	1.683	0.155	1.517
80	0.167	1.839	0.162	1.683
100	0.168	1.954	0.166	1.805
120	0.167	2.043	0.167	1.9
140	0.166	2.116	0.168	1.978
160	0.165	2.178	0.167	2.043
180	0.163	2.231	0.167	2.099
200	0.161	2.277	0.166	2.148
220	0.159	2.319	0.164	2.192

Верхняя строчка предполагает неизменный средний заработок больше 15 тысяч рублей во втором и третьем столбцах и больше 20 тысяч рублей в четвертом и пятом. Вторая и четвертая колонки показывают увеличение суммы сбора налога по сравнению с равномерной шкалой, дающей результат Q=0.13. Пересчет по формулам (2) дает соответствующее значение среднеквадратичного отклонения σ. Эту колонку мы сравниваем с известными статистическими данными в других статьях. Заметим, что с ростом доли Q собираемая сумма сначала увеличилась, а затем уменьшилась. Отмечен максимум возможной доли сбора.

Исследуем теоретически это необычное явление. Оно связано с возможностью логнормального распределения.

Особенности логнормального распределения и косвенное определение возможности появления нетрудовых доходов

Существует мнение, что эффективность введения прогрессивной шкалы подоходного налога зависит от представительности среднего класса в стране. Говоря точным языком, нужен анализ изменения суммы сбора налога в зависимости от параметра, характеризующего разброс значений доходов населения, — σ. Анализ таблицы показывает, что сумма доли дохода, собираемого по нашему примеру, сначала растет, а за-

тем убывает с увеличением параметра, характеризующего разброс легальных доходов. Бесспорно, что увеличение математического ожидания доходов пропорционально повлечет увеличение суммы сбора налога. Зависимость от величины σ более сложная (2). Для определения границ изменения суммы сбора налога в зависимости от параметра, определяющего разброс, воспользуемся правилом «трех сигм» для $\ln x$. Имеем неравенство $\ln x \le \mu + 3\sigma$, или $x \le \exp(\mu + 3\sigma)$**.** В относительном измерении к среднему доходу по формуле (2) получаем $x/\mu^* \le \exp\left(\sigma(3 - \sigma/2)\right)$. Максимум параболы $\sigma\left(3 - \sigma/2\right)$ достигается в точке $\sigma = 3$ и равен 4.5 . Граница относительного роста:

$$x/\mu^* \le \exp\left(\sigma(3 - \sigma/2)\right) \le \exp(4.5) \approx 90 . \qquad (3)$$

Для легальных доходов, распределенных по логнормальному закону, сумма дохода не должна превосходить среднюю величину дохода в 90 раз. Вернее, вероятность такого события почти равна единице. Так как согласно работам [1,2] именно логнормальное распределение характеризует легальные доходы российского населения в настоящее время, то превышение этой границы можно считать косвенным указанием на возможные нетрудовые доходы рассматриваемого физического лица.

Графическая иллюстрация эффективности модели

Проиллюстрируем некоторые значения таблицы, сопоставляя их с известными статистическими данными [2].

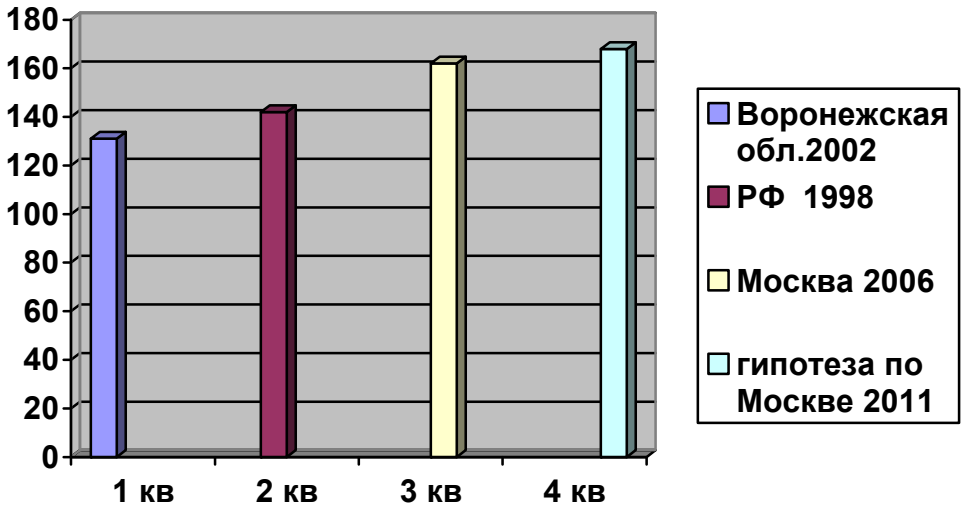


Рис. 2. Диаграмма изменения доли собираемого налога в зависимости от параметра σ

Высота показателей диаграммы рис. 2 соответствует доле собираемого налога. Значения параметра σ соответствуют статистическим данным работ [1,2]. Разброс по данным 2002 г. по Воронежской области $\sigma \approx 0{,}8$; согласно таблице, доля налога составляет $Q \approx 0{,}131$. Это чуть больше, чем при равномерной шкале. Средний разброс по РФ на 1998 г. $\sigma \approx 1{,}3$, доля налога $Q \approx 0{,}142$. Параметр, характеризующий разброс в доходах на 2006 г. по Москве $\sigma \approx 1{,}5$; доля налога $Q \approx 0{,}162$. Прогноз на 2011 г. по

Москве $\sigma \approx 2$; доля налога $Q \approx 0{,}168$. Это максимально возможное значение для шкалы, рассматриваемой в работе.

Выводы

Введение прогрессивной шкалы существенно не увеличит сбор налога для страны, в которой легальные доходы распределены по логнормальному закону. По-видимому, в таких малых странах, как Дания, закон распределения доходов не является логнормальным, а скорее приближается к равномерному закону, о чем свидетельствует и малое для этой страны значение коэффициента Рейнбоу. Тем не менее, введение предлагаемой прогрессивной шкалы позволит полностью освободить малоимущее население от налога, снизив социальное напряжение, и при этом доля сбора налога даже увеличится.

СПИСОК ЛИТЕРАТУРЫ

1. Скрыль С.В., Тростянский С.Н. Безопасность социоинформационных процессов: теория синтеза прогностических моделей: монография. — Воронеж: ВИ МВД России, 2008. —154 с.

2. Колмаков И.Б. Прогнозирование показателей дифференциации денежных доходов населения // Проблемы прогнозирования. — 2006. — №1. — С.136—162.

СВЕДЕНИЯ ОБ АВТОРАХ:

Горлов Сергей Кузьмич. Кандидат технических наук, доцент.
Тел. 8(473) 2384523.

Родин Владимир Александрович. Профессор кафедры высшей математики Воронежского института МВД России. Доктор физико-математических наук, профессор.
Воронежский институт МВД России.
E-mail: rodin_v@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. 89107499831.

Gorlov Sergey Kuzmich. The candidate of technical sciences, assistant professor .
Work address: Russia, 394065, Voronezh. Tel. 8(473) 2384523.

Rodin Vladimir Alexandrovich. Professor of High Mathematics chair. The doctor of physical and mathematical sciences, professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 89107499831.

Ключевые слова: математические модели налогообложения; функция стохастического распределения; модель подоходного налога.

Key words: mathematical models of the taxation;function of stochastic distribution;surtax model; check of stochastic hypotheses.

УДК 519.86

П.А. Леонтьев,
Пермский институт ФСИН России

А.П. Рыбаков,
доктор физико-математических наук, профессор, Пермский национальный исследовательский политехнический университет

С.А. Петров,
кандидат технических наук

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЧРЕЗВЫЧАЙНОГО ОБСТОЯТЕЛЬСТВА НА ОБЪЕКТАХ ПЕНИТЕНЦИАРНОЙ СИСТЕМЫ ПОСРЕДСТВОМ МЕТОДА ЛОГИКО-ВЕРОЯТНОСТНОГО ИСЧИСЛЕНИЯ

MATHEMATICAL MODELLING OF EMERGENCY SITUATIONS IN CORRECTIONAL FACILITIES BY MEANS OF LOGIC-AND-PROBABILISTIC METHOD OF CALCULUS

Приводится пример использования математического аппарата для расчета надежности систем охраны периметров учреждений уголовно-исполнительной системы.

The article views the example of application of mathematical apparatus for the evaluation of reliability of the systems of custody of correctional facilities perimeter.

Под чрезвычайными обстоятельствами понимаются происшедшие события, существенно влияющие на жизнедеятельность людей и общества и требующие принятия специальных мер по защите жизни, здоровья, прав и свобод граждан, материальных и иных ценностей от уничтожения, повреждения и по восстановлению нормальной работы.

Чрезвычайные обстоятельства в уголовно-исполнительной системе — это особо опасные события, происшедшие (происходящие) в учреждениях уголовно-исполнительной системы (УИС), вызванные явлениями криминального свойства и требующие принятия незамедлительных мер для их пресечения или ликвидации.

Побег осужденных из-под охраны относится к чрезвычайному обстоятельству.

Охрана объектов уголовно-исполнительной системы, предназначенных для содержания и труда осужденных, и других УИС осуществляется специальными подраз-

делениями уголовно-исполнительной системы, создаваемыми для этих целей при учреждениях, исполняющих наказания [1].

Для охраны объектов пенитенциарной системы специальными подразделениями создаются системы охраны, одним из показателей которых является надежность. Повышение надежности систем охраны является приоритетным направлением развития УИС. Но до настоящего времени попыток численно выразить величину надежности данных систем для анализа их эффективности не принималось.

В данной работе приведен пример применения метода логико-вероятностного исчисления для создания математической модели чрезвычайного обстоятельства на объектах пенитенциарной системы.

Пусть Y(X) — логическая функция, описывающая функционирование системы охраны. Тогда $Y(X_1 \ldots X_i); i \in N$ — функция опасности (совершения побега), где X_i — событие, нарушающее работу системы охраны (невыдача тревожного сигнала датчиком обнаружения, несвоевременное прибытие резервной группы и т.д.). Минимальная совокупность событий X_i (МСС), приводящая к побегу, МСС $=\wedge X_i$; $i \in N$. Логическая функция, описывающая работу системы охраны при совершении побега, представляет собой дизъюнкцию МСС $Y(X_1 \ldots X_i)=\vee[\wedge X_i]$.

Но логические функции не дают количественной оценки надежности системы охраны. Перейдем к вероятностной функции $F(Y)=P\{Y(X_1 \ldots X_i)=1\}$, характеризующей возможность невыполнения системой охраны своей функции. Для перевода $Y(X_1 \ldots X_i)$ необходимо привести её в одну из форм: совершенную дизъюнктивную нормальную форму (СДНФ); ортогональную дизъюнктивную нормальную форму (ОДНФ); бесповторную функцию в базисе конъюнкция — отрицание. Затем произведем замену: X_i заменим на $P(X_i=1)=R_i$, а $\overline{X}_i$ заменим на $P(\overline{X}_i = 1) = 1 \quad R_i$, где R_i — вероятность наступления события X_i [2].

Величина, противоположная вероятностной функции F(Y), характеризует уровень надежности охраны $Z(Y)=1-F(Y)$.

Рассмотрим систему защиты объекта УИС, состоящую из:

- нулевого рубежа обнаружения;
- часовых на периметре;
- первого рубежа обнаружения;
- второго рубежа обнаружения;
- резервной группы караула.

К совершению побега приводят инициирующие события, приведенные в таблице.

Составляем функцию опасного состояния системы (совершение побега). На рисунке видно, что побег будет совершен если:

- ни один из рубежей обнаружения не выдаст сигнал тревоги и часовой не заметит нарушителя $X_1 \wedge X_2 \wedge X_3 \wedge X_4$;
- какой-либо из рубежей обнаружения выдаст сигнал тревоги или часовой обнаружит нарушителя, но при этом не задержит нарушителя и резервная группа караула не своевременно прибудет к месту побега $(\overline{X}_1 \vee \overline{X}_2 \vee \overline{X}_3 \vee \overline{X}_4) \wedge X_5 \wedge X_6$.

Получаем функцию совершения побега:

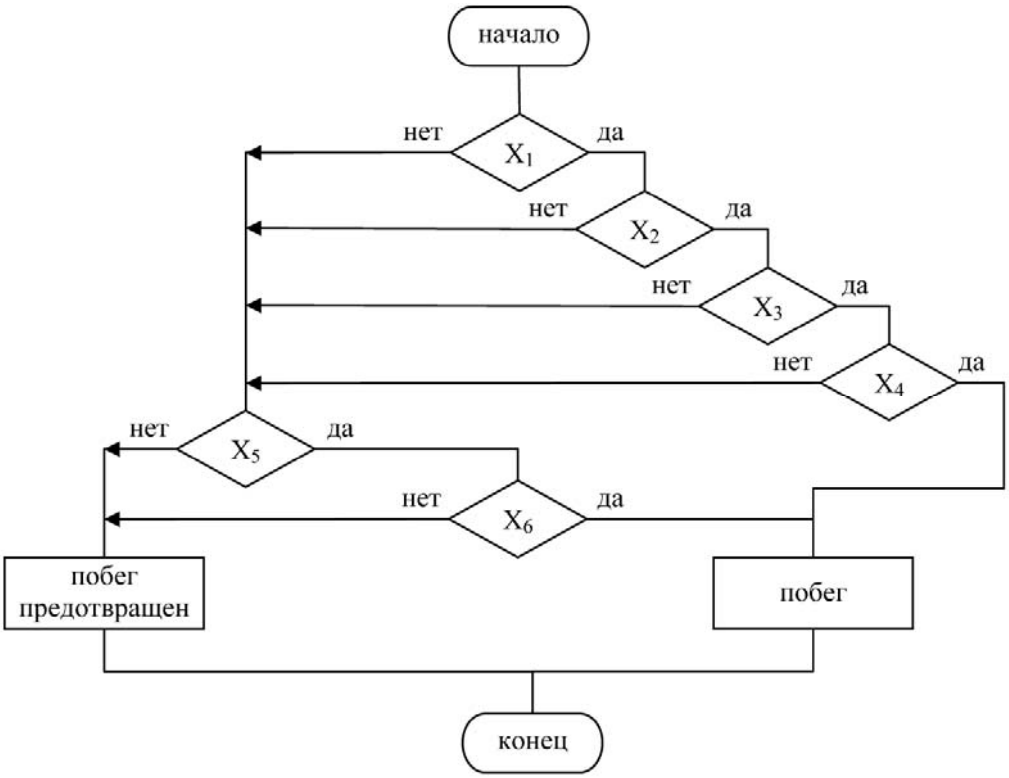
$$Y(X_1 \ldots X_6) = [X_1 \wedge X_2 \wedge X_3 \wedge X_4] \vee [(\overline{X}_1 \vee \overline{X}_2 \vee \overline{X}_3 \vee \overline{X}_4) \wedge X_5 \wedge X_6]. \quad (1)$$

Инициирующие события, приводящие к совершению побега

Инициирующее событие	Обозначение	Вероятность события
Необнаружение нарушителя нулевым рубежом охраны	X_1	R_1
Необнаружение нарушителя первым рубежом охраны	X_2	R_2
Необнаружение нарушителя вторым рубежом обнаружения	X_3	R_3
Необнаружение нарушителя часовым наблюдательной вышки	X_4	R_4
Несвоевременное прибытие резервной группы к месту совершения побега	X_5	R_5
Незадержание осужденного часовым наблюдательной вышки	X_6	R_6

Представим выражение (1) в дизъюнктивной нормальной форме:

$$Y(X_1...X_i) = X_1X_2X_3X_4 \vee \overline{X_1}X_5X_6 \vee \overline{X_2}X_5X_6 \vee \overline{X_3}X_5X_6 \vee \overline{X_4}X_5X_6 . \qquad (2)$$



Алгоритм событий, приводящих к совершению или предотвращению побега

Из этого выражения хорошо видны все пути развития опасности:

$MCC_1 = X_1X_2X_3X_4$; $MCC_2 = \overline{X_1}X_5X_6$; $MCC_3 = \overline{X_2}X_5X_6$; $MCC_4 = \overline{X_3}X_5X_6$; $MCC_5 = \overline{X_4}X_5X$.

Инвертируя ранее полученное выражение (1) (правило де Моргана [3]), получим функцию безопасности системы:

$$\overline{Y}(X_1...X_6)=\overline{[X_1 \wedge X_2 \wedge X_3 \wedge X_4] \vee [(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \wedge X_5 \wedge X_6]}=$$

$$=\overline{X_1X_2X_3X_4} \wedge \overline{(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4})X_5X_6}=$$

$$=[\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}] \wedge \overline{[(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \vee \overline{X_5} \vee \overline{X_6}]}=$$

$$=(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4})\overline{(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4})} \vee (\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4})X_5 \vee (\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4})X_6=$$

$$=\overline{X_1}\,\overline{X_5} \vee \overline{X_2}\,\overline{X_5} \vee \overline{X_3}\,\overline{X_5} \vee \overline{X_4}\,\overline{X_5} \vee \overline{X_1}\,\overline{X_6} \vee \overline{X_2}\,\overline{X_6} \vee \overline{X_3}\,\overline{X_6} \vee \overline{X_4}\,\overline{X_6}\,. \qquad (3)$$

Функция безопасности представляет собой конъюнкцию вариантов предотвращения побега (ВПП).

Для перехода к вероятностной функции побега с объекта представим выражение (1) в виде бесповторной булевой функции в базисе конъюнкция — отрицание:

$$Y(X_1..X_6)=(X_1 \wedge X_2 \wedge X_3 \wedge X_4) \vee [(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \wedge X_5 \wedge X_6]=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4) \vee [(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \wedge X_5 \wedge X_6]}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{[(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \wedge X_5 \wedge X_6]}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{[(\overline{X_1} \vee \overline{X_2} \vee \overline{X_3} \vee \overline{X_4}) \vee \overline{X_5} \vee \overline{X_6}]}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{[(X_1 \wedge X_2 \wedge X_3 \wedge X_4) \vee \overline{X_5} \vee \overline{X_6}]}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge (X_1 \wedge X_2 \wedge X_3 \wedge X_4) \vee \overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{X_5} \vee \overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{X_6}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge (\overline{X_5} \vee \overline{X_6})}=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge \overline{(\overline{X_5} \vee \overline{X_6})}}=$$

$$=\overline{\overline{(X_1 \wedge X_2 \wedge X_3 \wedge X_4)} \wedge (X_5 \wedge X_6)}. \qquad (4)$$

Преобразуем формулу логической алгебры (4) в вероятностную функцию $F(Y)=P\{Y(X_1 \ldots X_6)=1\}$, при этом X_i заменяем на R_i, а $\overline{X_i}$ — на $Q_i=1-R_i$, получаем формулу расчета вероятности совершения побега:

$$F(Y)=1-(1-R_1R_2R_3R_4)(1-R_5R_6). \qquad (5)$$

Таким образом, надежность охраны равна

$$Z(Y)=1-F(Y)=(1-R_1R_2R_3R_4)(1-R_5R_6). \qquad (6)$$

Если принять за расчетные показатели следующие значения вероятностей:

$R_1=0{,}1$ (среднестатистическая вероятность необнаружения нарушителя датчиком);

$R_2=0{,}1$ (среднестатистическая вероятность необнаружения нарушителя датчиком);

$R_3=0{,}1$ (среднестатистическая вероятность необнаружения нарушителя датчиком);

$R_4=0{,}4$ (среднестатистическая вероятность необнаружения нарушителя часовым на наблюдательной вышке);

$R_5=0{,}2$ (среднестатистическая вероятность незадержания нарушителя резервной группой);

$R_6=0{,}4$ (среднестатистическая вероятность незадержания нарушителя часовым), то при таких данных вероятность совершения побега $F(Y)=0{,}08$, соответственно надежность охраны $Z(Y)=0{,}92$.

Хотелось бы отметить, что данный алгоритм побега является приближенным и не охватывает все аспекты, влияющие на надежность охраны, но позволяет, основываясь на методе ЛВИ, провести глубокие исследования в области надежности объектов охраны.

ЛИТЕРАТУРА

1. Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: Закон РФ от 21.07.1993 №5473-1 (ред. от 06.11.2011). — Ст. 12.

2. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. — СПб.: Бизнес-пресса, 2004. — 216 с.

3. Колмогоров А.Н., Драгалин А.Г. Математическая логика. — 3-е изд., стереотип. — М.: Ком. Книга, 2006. — 240 с.

СВЕДЕНИЯ ОБ АВТОРАХ:

Леонтьев Павел Александрович. Преподаватель кафедры организации охраны и конвоирования в уголовно-исполнительной системе.
Пермский институт ФСИН России.
E-mail: leontjevpavel@yandex.ru
Россия, 614012, Пермь, Карпинского, 125. Тел. (342) 228-65-04 (169).

Рыбаков Анатолий Петрович. Профессор кафедры общей физики. Доктор физико-математических наук, профессор.
Пермский национальный исследовательский политехнический университет.
E-mail: anatryb@yandex.ru
Россия, 614990, Пермь, Комсомольский проспект, 29. Тел. (342) 219-82-12.

Петров Семен Александрович. Преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: petrovsemen1@mail.ru
Россия, 394065, г.Воронеж, проспект Патриотов, 53. Тел. (473) 2731-372.

Leontyev Pavel Alexandrovich. Lecturer of the chair of Organization of Guard and Escort in Penal System.
Perm Institute of the Federal Penal Service.
Work address: Russia, 614012, Perm, Karpinsky Str., 125. Tel. (342) 228-65-04 (169).

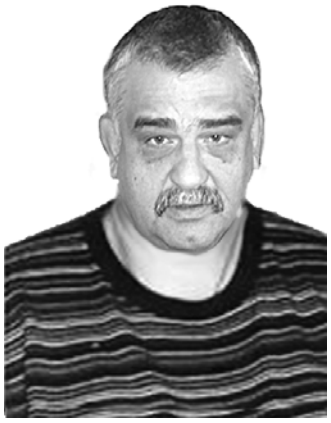
Rybakov Anatoly Petrovich. Professor of the chair of General Physics. Doctor of physics and mathematics, professor.
Perm State National Research Polytechnical University.
Work address: Russia, 614990, Perm, Komsomolsky Avenue, 29. Tel. (342) 219-82-12.

Petrov Simeon Alexandrovich. Lecturer of the chair of Infocommunication Systems and Technologies. Candidate of technical sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2731-372.

Ключевые слова к статье: чрезвычайное обстоятельство; система охраны;надежность; вероятность.

Key words: situation of emergency; security system; reliability;probability.

УДК 343.8



Е.А. Рогозин,
доктор технических наук, доцент,
Воронежский государственный
технический университет

Д.Ф. Хисамов,
кандидат технических наук,
Кубанский институт информзащиты

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ НЕПРИЕМА ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ В ДИСКРЕТНЫХ КАНАЛАХ С ПАМЯТЬЮ

MATHEMATICAL MODEL OF UNDERTENTION PSEUDO-CASUAL SEQUENCE IN THE DISCRETE CHANNELS OF MEMORY

Разработан математический аппарат для оценки вероятности неприема псевдослучайной последовательности (ПСП) в биномиальных и составных каналах с релеевскими замираниями при синхронизации по методу зачетного отрезка. Проведены сравнительные оценки синхронизации датчиков ПСП в указанных каналах для различных периодов псевдослучайной последовательности и качества канала связи. На основе расчетов даны практические рекомендации по реализации систем синхронизации датчиков ПСП на каналах с памятью.

The mathematical device for an estimation of probability undertention pseudo-casual sequence (PCS) in binomial and compound channels with relay fades is developed at synchronization on a method of a test piece. Comparative estimations of synchronization of gauges APCS in the specified channels for the various periods of pseudo-casual sequence and quality of a liaison channels are carried out. On the base of calculations practical recommendations on realization of systems of synchronization of gauges APCS in memory channels are given.

Введение

Известные математические модели неприменимы для расчета синхронизации ПСП на нестационарных каналах низкого качества с релеевскими замираниями. Даже при биномиальном распределении ошибок в каналах ДСК они находят ограниченное применение при больших периодах ПСП, так как в формулах фигурирует факториал от периода ПСП. В специальных системах связи для защиты составных сигналов период ПСП выбирается необозримо большим, поэтому найдем аналитические выражения для оценки синхронизации датчиков ПСП специальных систем связи на нестационарных

каналах связи с релеевскими замираниями и биномиальных каналах ДСК и произведем расчеты для каналов различного качества при различных периодах ПСП.

Вывод вероятности неприема ПСП в составном канале с переменными параметрами при разнесенном приеме с автовыбором

Предположим, что параметр канала не успевает измениться на каком-то интервале времени, то есть: $\mu_1=\mu_2=\ldots=\mu_n=\mu$.. Такое условие приближенно выполняется, например, для коротковолновых (КВ) каналов, если $n\cdot\tau_0 \le 0.5$с, или для тропосферных каналов при условии $n\cdot\tau_0 \le 0.05$с. Соответственно с учетом скорости передачи по каналу получим для КВ канала $n \le 0.5\cdot U$ и тропосферного $n \le 0{,}05\cdot U$, где U — скорость передачи в канале; τ_0 — длительность элементарного импульса. Учитывая, что в КВ канале максимальная скорость передачи равна 300 бодам, легко определить максимальную длину блока, в котором параметр μ_i можно считать постоянным, $n \le 60$, или для тропосферного канала, где обычно U=1200—2000000 бод, $n \le 100000$.

Следовательно, сделанное предложение будет справедливо для систем синхронизации с «зачетным отрезком», длина зачетного отрезка (ЗОТ) в которых $n \le 60$ для КВ каналов и $n \le 100000$ для тропосферных каналов. Или, учитывая [1], что длина зачетного отрезка складывается и равна: $к+m \le n < N=2^k-1$, где $к$ — длина ЛРР; m — емкость счетчика совпадений, можем записать:

для КВ канала: $k+m \le n \le 60$ (1)

для тропосферного канала: $k+m \le n \le 100000$. (2)

Для нахождения вероятности $P_{\text{н}}$ опишем модель канала синхронизации по зачетному отрезку при сделанных предположениях. Для этого разобьем ПСП на интервале анализа N на блоки из n элементов. Получим $Z=N/n$ не пересекающихся зачетных отрезков. Будем считать, что зачетные отрезки независимы между собой [1, 2] и на длине ЗОТ, по определению составного канала с переменными параметрами μ, постоянно. Тогда для вероятности неприема ПСП будет справедливо равенство:

$$P_{н}^{рз}=\left(1-P_{бо}(n)\right)^{Z}, \tag{3}$$

где $P_{бо}(n)$ — вероятность безошибочного приема блока из n символов в составном КПП.

Для вероятности правильного приема можем записать:

$$P_{пп}^{рз}=1-P_{н}^{рз}. \tag{4}$$

Известно [4], что вероятность безошибочного приема блока из n символом в составном канале находится как:

$$P_{\text{бо}}(n)=P_{\text{бо}}^{Q}(n)=Q\sum_{i=0}^{Q-1}(-1)^{i}\cdot C_{Q-1}^{i}\cdot S_{n}^{(i+1)}, \tag{5}$$

где

$$\text{S}_{\text{n}}^{(\text{i}+1)}=\frac{2^{-\text{n}}+\frac{\text{H}^2}{2}\cdot\text{n}\cdot\text{S}_{\text{n}-1}^{\text{i}+1}}{\text{k}+1+\frac{\text{H}^2}{2}\cdot\text{n}};$$

$$\text{S}_{0}^{\text{i}+1}=1/(\text{k}+1);$$

Q — число ветвей разнесения.

Подставляя (5) в (3), получим:

$$P_{\text{н}}^{\text{рз}} = \left(1 - Q \cdot \sum_{i=0}^{Q-1} (-1)^i \cdot C_{Q-1}^i \cdot S_n^{(i+1)}\right)^Z . \quad (6)$$

Вывод вероятности неприема ПСП в биномиальном канале

По аналогии с составным каналом КПП для вероятности неприема ПСП в биномиальном канале ДСК будет справедлива оценка:

$$P_н^б = \left[1 - (1 - P)^n\right]^Z . \quad (7)$$

А для вероятности правильного приема можем записать:

$$P_{пп}^б = 1 - P_н^б , \quad (8)$$

где $P=1/(2+H^2)$,

$H^2 = \frac{a^2}{\sigma^2}$ — отношение средней энергии элемента сигнала на входе приемника к спектральной плотности помехи.

Оценим вероятность неприема $P_н$ в составном КПП при разнесенном приеме с автовыбором и сравним полученные результаты с синхронизацией ПСП в эквивалентном биномиальном канале.

Сравнительная оценка вероятности неприема ПСП в биномиальном и составном КПП при разнесенном приеме с автовыбором

По формулам (6), (4), (7), (8) для различных значений Q, n и N были произведены сравнительные расчеты на ПЭВМ. Результаты расчетов показаны на рис.1 в виде графиков функций: $P_{\text{н}}^{\text{рз}} = \varphi(n)$; $P_{\text{н}}^{\text{б}} = \varphi(n)$ и на рис. 2 в виде графиков функций: $P_{\text{пп}}^{\text{рз}} = \varphi(n)$; $P_{\text{пп}}^{\text{б}} = \varphi(n)$.

Анализ графиков рис.1 показывает, что вероятность неприема $P_н$ в составном КПП гораздо меньше, чем в эквивалентном биномиальном канале. Причем при увеличении H^2 эта разница возрастает. Например, для N=127, n=20, Q=1 и H^2=8 вероятность неприема в составном канале $P_н^{рз}$ на 3 десятичных порядка меньше, чем вероятность неприема в эквивалентном биномиальном канале $P_н^б$, а при H^2=18 эти вероятности различаются на 4 десятичных порядка. С увеличением же n эта разница убывает. Например, если для N=127, Q=1, H^2=18 и n=20 вероятность неприема в составном канале меньше вероятности неприема в биномиальном на 4 порядка, то при n=50 эта разница убывает и составляет всего лишь два десятичных порядка. При увеличении n вероятность неприема в составном канале возрастает быстрее, чем в биномиальном. То есть, синхронизация в составном канале более критична к выбору длины зачетного отрезка n, чем в эквивалентном биномиальном канале. Однако при одинаковых вероятностях неприема вероятность ложной синхронизации в составном КПП будет меньше, чем в биномиальном канале, за счет удлинения самого зачетного отрезка. Действительно, из графиков видно, что при $\text{Р}_{\text{н}}^{\text{рз}} = \text{Р}_{\text{н}}^{\text{б}} = 10^{-2}$ в биномиальном канале n=11, а в составном n=40.

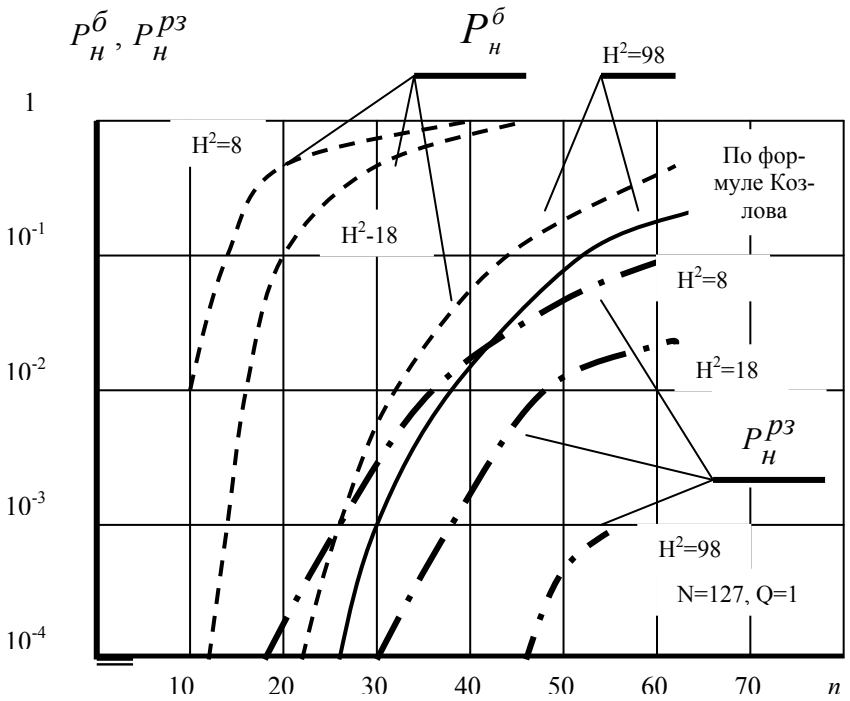


Рис. 1. Вероятность неприема ПСП в биномиальном и в составном каналах связи

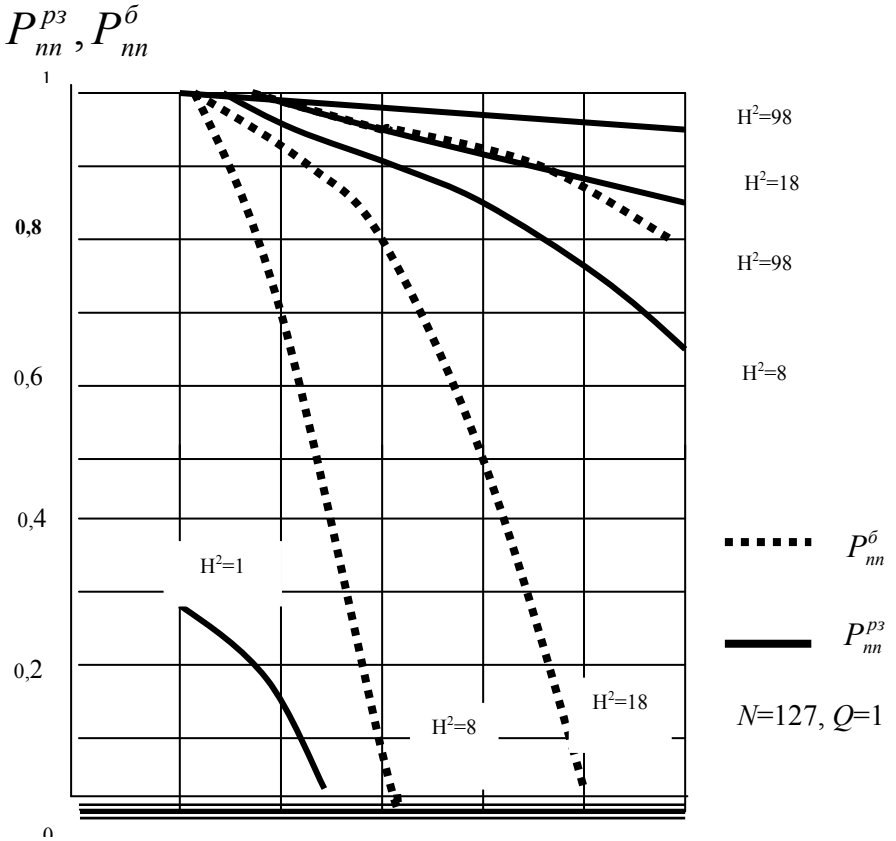


Рис. 2. Оценка вероятности правильного приема ПСП в биномиальном и в составном каналах связи

Следовательно, в составном канале быстрее можно войти в синхронизм. Это преимущество хорошо видно на рис. 2. С увеличением длины зачетного отрезка n вероятность правильного приема в составном канале $P_{пп}^{рз}$ убывает значительно медленнее, чем вероятность правильного приема в эквивалентном биномиальном канале $P_{пп}^{б}$. То есть в составном КПП вероятность правильного приема ПСП сохраняется на достаточно высоком уровне даже при увеличении n в несколько раз. Расчеты показывают, что с увеличением ветвей разнесения Q или периода ПСП N качественные показатели системы синхронизации ПСП в составном КПП резко улучшаются. То есть вероятность неприема стремится к нулю, а вероятность правильного приема ПСП — к единице ($\mathrm{P}_{\mathrm{н}}^{\mathrm{рз}} \to 0$, а $\mathrm{P}_{\mathrm{пп}}^{\mathrm{рз}} \to 1$), см. рис.3. Расчеты показывают, что прием с разнесением и автовыбором целесообразно использовать при H^2<8, так как на таких каналах эффективность одиночного приема резко падает, например, из рис.2 видно, что при N=127, Q=1 и H^2=1 даже при n=10 вероятность правильного приема ПСП $P_{пп}^{рз} < 0{,}5$.

Необходимо отметить, что при данной методике расчета не учитываются чистые интервалы длиной в n знаков, появляющиеся на стыках между смежными зачетными отрезками. Следовательно, (3) и (7) дают верхнюю оценку для $P_{\mathrm{н}}$. Для сравнения на рис.1 показан график вероятности неприема ПСП, как функция от длины зачетного отрезка $P_{\mathrm{н}}^{\mathrm{б}} = \varphi(n)$, рассчитанной по точной формуле Козлова [3].

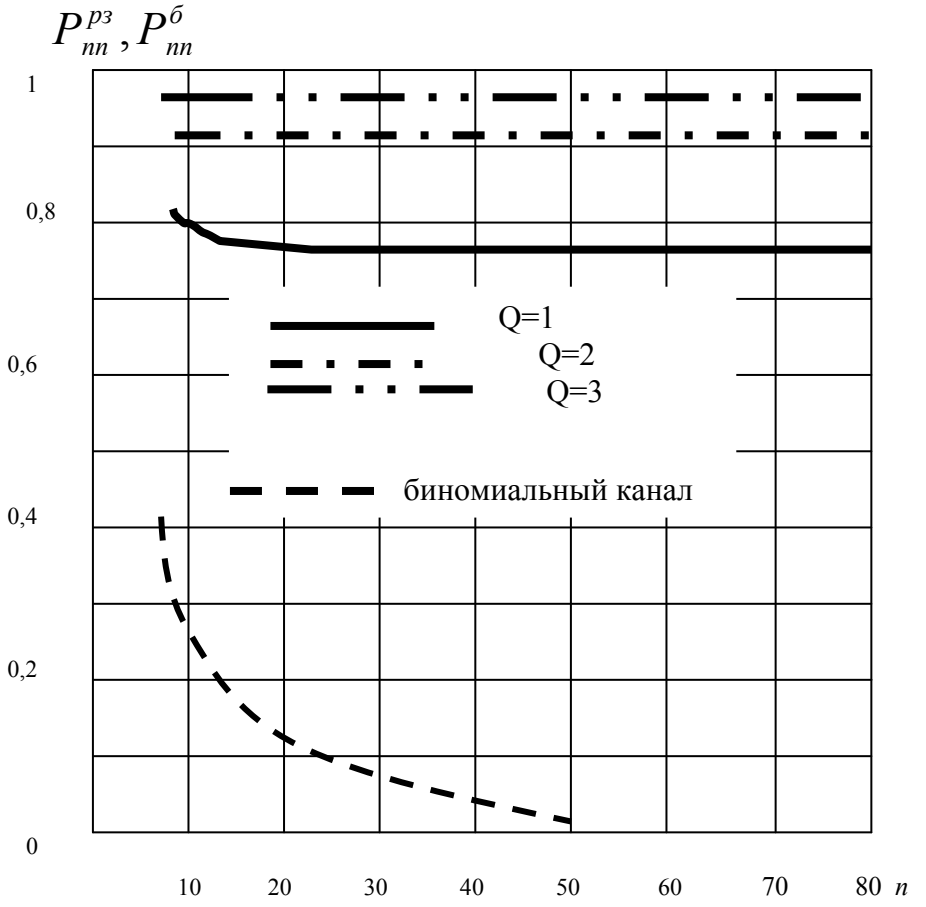


Рис. 3. Вероятность правильного приема ПСП в биномиальном канале и квазибиномиальном канале с ветвями разнесения Q=1, Q=2, Q=3

Видно, что кривая $P_{\text{н}}^{\text{б к}} = \varphi(n)$ при одинаковых H^2 идет ниже кривой вероятности неприема ПСП в эквивалентном биномиальном канале $P_{\text{н}}^{\text{б}} = \varphi(n)$, но вероятность неприема больше, чем в эквивалентном составном КПП $P_{н}^{рз}$. То есть хорошо сохраняется общая закономерность изменения вероятности неприема в биномиальном канале, рассчитанной по формуле Козлова и по формуле (7), полученной в данной работе, что указывает на верность предыдущих выводов относительно сравнительного анализа синхронизации ПСП в составном и биномиальных каналах связи.

В отличие от биномиального канала, оценка (6) для составного канала будет мало отличаться от истинной. Действительно в составном канале вероятность появления ошибок на g фиксированных местах при одинаковых соотношениях сигнал/помеха H^2 больше, чем в биномиальном, и уменьшается при раздвижении единиц в образце ошибок [4], то есть можем записать:

$$P\left(e_{i_g} / i_g \geq n\right) < P\left(e_{i_g} / i_g < n\right), \tag{9}$$

где $P\left(e_{i_g} / i_g \geq n\right)$ — вероятность появления образца ошибок e_{i_g} с расположением единиц на фиксированных местах, при условии, что расстояние между смежными единицами $\geq n$;

i_g — расстояние между смежными единицами в образце ошибок e_{i_g}.

Из (9) видно, что вероятность появления чистого интервала из n символов между смежными ЗОТ будет меньше вероятности его непоявления, то есть существенного увеличения вероятности правильного приема ПСП в составном КПП $P_{пп}^{рз}$ за счет неучтенных ЗОТ ожидать не приходится. В частности, расчеты показывают, что при n=50 погрешность за счет неучтенных ЗОТ составит примерно два процента.

Вывод

В заключение отметим, что полученные результаты можно обобщить на КПП с произвольными параметрами канала μ_i. Известно [4], что $P_{н}^{рз}$ не зависит от конфигурации ошибок в зачетном блоке, а определяется лишь появлением хотя бы одной ошибки. На основании этого с достаточной уверенностью можно утверждать, что количественные результаты по синхронизации ПСП, полученные для составных КПП позволят повысить качество проектирования устройств синхронизации ПСП специальных систем связи.

ЛИТЕРАТУРА

1. Хисамов Д.Ф. Расчет вероятности ложной синхронизации псевдослучайной последовательности по методу зачетного отрезка в биномиальных каналах связи // Сборник научных работ СПб ВМИ. — Санкт-Петербург, 2002. — С. 5—7.

2. Хисамов Д.Ф. Граничные оценки вероятности синхронизации псевдослучайной последовательности на каналах с произвольным распределением ошибок // Математика в XXI веке: материалы международного конгресса 25—28 июня 2003 г. — Новосибирск: Академгородок, 2003. http://www.sbras.ru/ws/ MMF-21/

3. Козлов А.Ф. О вычислении вероятности неприема рекуррентного сигнала // Сборник научных трудов ЦНИИИС МО СССР. — М., 1964. — № 4.

4. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. — М.: Связь, 1975.

СВЕДЕНИЯ ОБ АВТОРАХ:

Рогозин Евгений Алексеевич. Профессор кафедры конструирования и производства радиоаппаратуры. Доктор технических наук, доцент.

Воронежский государственный технический университет.

E-mail: EvgeniRogozin@yandex.ru

Россия, 394042, г. Воронеж, Московский проспект, 159. Тел.8(473) 246-26-30.

Хисамов Денис Франгизович. Доцент кафедры комплексной защиты информации. Кандидат технических наук.

Кубанский институт информзащиты.

E-mail: kiiz@rambler.ru.

Россия, 350010, г. Краснодар, ул. Зиповская, 5. Тел. 8(861)252-30-31.

Rogozin Evgeni Alekseevich. Professor of the chair of designing and production of radio equipment. Doctor of technical sciences, assistant professor.

Voronezh State Engineering University.

Work address: Russia, 394042, Voronezh, Moscow Prospect, 159. Tel. 8(473) 246-26-30.

Khisamov Denis Frangizovich. Assistant professor of the chair of complex information protection. Candidate of technical sciences.

Kuban Institute of Information Protection.

Work address: Russia, 350010, Krasnodar, Zipovskaja Str., 5. Tel. 8(861)252-30-31.

Ключевые слова: канал с релеевскими замираниями; биномиальный канал; синхронизация ПСП.

Key words: channels with relay fades; binomial channel; PCS synchronization.

УДК 681.327.8

О.В. Пьянков,
кандидат технических наук, доцент

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

РАЗРАБОТКА ПРАВИЛ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ЭКСТРАПОЛЯЦИИ ЭКСПЕРТНЫХ ОЦЕНОК

DEVELOPMENT OF THE DECISION MAKING RULES ON THE BASIS OF EXPERT EVALUATIONS EXTRAPOLATION

Рассматривается возможность разработки правил принятия решений по выбору действий органов внутренних дел. Предлагается правило принятия решений, использующее формализацию нечётких оценок экспертов и их экстраполяцию на основе метода наименьших квадратов.

The possibility of the decision rules development for selection of the acts of the Law Enforcement Agencies is considered. Rule making, using the formalization of fuzzy expert evaluations and their extrapolation based on the method of least squares is proposed.

Введение

Вопросы обеспечения безопасности и охраны правопорядка всегда являлись первостепенными задачами органов внутренних дел. Развитие современных информационных технологий, аппаратно-программных комплексов и средств связи позволяет не только осуществлять удаленный мониторинг мест массового пребывания граждан, обстановку на дорогах и т.п. в рамках реализации программы «Безопасный город», но и накапливать значительные объемы данных для разработки правил принятия решений [1]. Разработка таких правил не только позволит осуществлять более обоснованное принятие решений при наличии соответствующего резерва времени, но, в первую очередь, поможет осуществить подготовку личного состава к действиям, в том числе и в кризисных ситуациях [2].

Реагирование на изменение ситуации в зоне мониторинга включает в себя оценку текущей ситуации и выбор действий органов внутренних дел. Описание возникающих ситуаций позволяет при привлечении экспертов определить наилучшие действия,

однако появление других ситуаций в новых условиях потребует повторного опроса экспертов, что практически невозможно выполнить в оперативном режиме. Соответственно, необходима разработка правил принятия, которые бы экстраполировали имеющиеся экспертные оценки на новые ситуации, особенно это важно при возникновении кризисных ситуаций [3]. Формализация этапов реагирования позволит разработать и применять правила принятия решений в служебной деятельности.

Оценка текущей ситуации

Использование составных элементов АПК «Безопасный город», таких как подсистема видеонаблюдения, подсистема экстренной связи «Гражданин-полиция», спутниковые навигационно-мониторинговые системы ГЛОНАСС или ГЛОНАСС/GPS, должно разумно сочетаться с другими подсистемами информационно-аналитического обеспечения деятельности органов внутренних дел. В этом случае и оперативная обстановка, и сводки происшествий за любой период, и другие сведения доступны сотрудникам комендантских отделений, дежурных частей, ситуационных центров непосредственно принимающих решения по выбору действий, направленных на поддержание общественной безопасности и охрану общественного порядка.

Для оценки ситуаций могут быть различные подходы [3], главным является возможность использования числовых показателей, характеризующих как качественные, так и количественные показатели. Другая особенность — возможность выделения набора главных характеристик для любой ситуации. Вполне естественно, что перечень ситуаций, с которыми сталкиваются органы внутренних дел, широк и разнообразен, но главное — конечен. Следовательно, для *типовых* ситуаций, встречающихся на практике, можно определить, исходя из накопленных данных, некоторые *типовые* характеристики, используемые для оценки ситуации при принятии решений. Например, такими характеристиками могут быть: площадь территории, на которой возникла ситуация; число участников (можно с разделением по категориям — жертва, преступник, свидетель и т.д.); число сотрудников нарядов, патрулей (пешие, на мото- или автотранспорте и т.д.), направленых к месту возникновения ситуации и т.д.

Таким образом, известными величинами при возникновении типовой ситуации s_i будут являться:

$H_i = \{h_{1i}, \quad h_{2i}, \quad ..., \quad h_{ni}\}$ — множество типовых характеристик ситуации;

$U_i = \{u_{1i}, \quad u_{2i}, \quad ..., \quad u_{mi}\}$ — множество условий, в которых происходит ситуация.

Обозначим через V_i свойства ситуации:

$$V_i = \{H_i, U_i\} = \{h_{1i}, \quad h_{2i}, \quad ..., \quad h_{ni}, u_{(n+1)i}, \quad u_{(n+2)i}, \quad ..., \quad u_{(n+m)i}\} = \{v_{1i}, \quad v_{2i}, \quad ..., \quad v_{ki}\},$$

где $k = m + n$.

Числовое значение свойства v_i будем обозначать как zv_i.

Тогда в результате определения набора типовых ситуаций $S = \{s_1, s_2, ..., s_r\}$ и анализа накопленных данных можно сформировать значительный эмпирический материал, по которому можно с привлечением экспертов разработать правила принятия решений.

Выбор действий

Принятие решений по выбору действий органов внутренних дел часто регламентируется нормативными правовыми документами как федерального, регионального, так и ведомственного уровня. Однако часто, особенно при возникновении крупных кризисных ситуаций, требуется определить первоочередные действия из множества альтернативных, соответствующих *i*-й ситуации.

Введём следующие обозначения:

D — множество всех действий, которые могут быть выполнены органами внутренних дел;

D_i — множество действий, которые могут быть выполнены органами внутренних дел в i-й ситуации, при этом $D_i \subseteq D$;

$r = |D_i|$ — мощность множества.

Тогда, рассматривая какую-либо i-ю ситуацию, эксперты могут для различных значений определять действие или набор действий, которые необходимо выполнить. Однако часто эксперты могут предложить действия лишь с некоторой степенью уверенности в его необходимости. Эту уверенность можно задать с помощью функции принадлежности μ_A, используемой в теории нечётких множеств [4].

Напомним, что нечеткое множество $A = \{(x, \mu_A(x))\}$ определяется математически как совокупность упорядоченных пар, составленных из элементов x универсального множества X и соответствующих степеней принадлежности $\mu_A(x)$ или непосредственно в виде функции $\mu_A: X \to [0, 1]$.

Введём для экспертов лингвистическую переменную «необходимость использования» действия $d_{ji} \in D_i$, которая будет принимать любые значения из конечного линейного упорядоченного множества X, состоящего из следующих элементов:

x_1 — очень сильная: действие необходимо выбрать;

x_2 — сильная;

x_3 — средняя: в данных условиях действие можно не выполнять;

x_4 — слабая;

x_5 — очень слабая: действие рекомендуется не применять.

Значения x_1 и x_4 в данном случае служат промежуточными элементами.

Тогда в результате анализа ситуации s_i с характеристиками zv_i эксперт может выбрать соответствующее значение $x_i \in X$ для каждого действия из D_i:

свойства ситуации *необходимость действия*

$$V_i = \{v_{1i},\ v_{2i},\ ...,\ v_{ki}\} \Rightarrow \text{Эксперт} \Rightarrow X_{s_i} = \{x_{1i},\ x_{2i},\ ...,\ x_{ri}\}.$$

Дальнейшая обработка результатов связана с получением количественных характеристик необходимости выбора данного действия, т.е. значений функции принадлежности $\mu_A(x_i)$. Не рассматривая в данном случае вид функции принадлежности (треугольная, трапециевидная и т.п.), отметим принципиальную возможность его определения известными методами [4] и получения набора M_{s_i} численных значений необходимости применения действия:

$$X_{s_i} = \{x_{1i},\ x_{2i},\ ...,\ x_{ri}\} \Rightarrow M_{s_i} = \{\mu(x_{1i}), \mu(x_{2i}), ..., \mu(x_{ri})\}.$$

В случае привлечения не одного, а группы экспертов имеется возможность статистической обработки полученных результатов известными методами [5].

Следует отметить, что, изменяя свойства рассматриваемой ситуации, можно получить разные наборы $M = \{M_{s_i}1,\ M_{s_i}2,\ \ldots\ M_{s_i}q\}$, которые позволят разработать правила принятия решений на основе экстраполяции экспертных оценок.

Экстраполяция экспертных оценок

Полученные в результате обработки экспертных оценок результаты можно использовать при возникновении новых ранее не встречавшихся свойств ситуации. Для этого необходимо определить такую функцию F_i, которая бы сопоставляла свойствам zv_i результаты экспертных оценок M_{s_i} : $F(\{zv_i\}) = M_{s_i}$. В самом простейшем случае такая функция может являться линейной свёрткой:

$$F(\{zv_i\}) = \sum_{j=1}^{k} \alpha_j \cdot (zv_i)_j = \mu(x_j).$$

Соответственно для определения всех значений функции принадлежности необходимо определить значения коэффициентов α_j, т.е. решить следующую систему уравнений:

$$\begin{cases} zv_{1i}\alpha_{11i} + zv_{2i}\alpha_{21i} + ... + zv_{ki}\alpha_{k1i} = \mu(x_1) \\ zv_{1i}\alpha_{12i} + zv_{2i}\alpha_{22i} + ... + zv_{ki}\alpha_{k2i} = \mu(x_2) \\ ... \\ zv_{1i}\alpha_{1ri} + zv_{2i}\alpha_{2ri} + ... + zv_{ki}\alpha_{kri} = \mu(x_r) \end{cases}, \quad (1)$$

или в матричной форме

$$zV_i \cdot [\alpha_{kr}]_i = M_{s_i}, \quad (1')$$

где zV_i — вектор-строка, составленный из числовых значений zv_i,

$[\alpha_{kr}]_i$ — матрица коэффициентов.

Однако составленная в таком виде (1) система имеет $k \cdot r$ неизвестных при наличии r уравнений, т.е. имеет решение при учёте только одного свойства ($k = 1$). Если такое свойство имеется, то можно этим и ограничиться, но следует отметить, что это встречается достаточно редко.

Рассмотрим возможные способы изменения системы (1) для определения искомой функции F_i.

Способ 1. Приведение zV_i и M_{s_i} к квадратичному виду (квадратной матрице).

Для этого необходимо выполнение условия $k = r$. Таким образом, в зависимости от первоначальных значений k и r, необходимо:

$k < r$ — либо уменьшить число рассматриваемых действий, либо ввести дополнительные свойства ситуации;

$k > r$ — либо уменьшить число рассматриваемых свойств, либо ввести дополнительные действия.

После этого дополнить систему (1) разными сочетаниями свойств ситуации и соответственно результатами экспертного опроса. При этом необходимо рассмотреть k различных линейно независимых сочетаний. Система уравнений примет вид:

$$\begin{pmatrix} zv_{11} & zv_{12} & ... & zv_{1k} \\ zv_{21} & zv_{22} & ... & zv_{2k} \\ ... & ... & ... & ... \\ zv_{k1} & zv_{k2} & ... & zv_{kk} \end{pmatrix}_i \cdot \begin{pmatrix} \alpha_{11} & \alpha_{12} & ... & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & ... & \alpha_{2k} \\ ... & ... & ... & ... \\ \alpha_{k1} & \alpha_{k2} & ... & \alpha_{kk} \end{pmatrix}_i = \begin{pmatrix} \mu_1(x_1) & \mu_1(x_2) & ... & \mu_1(x_k) \\ \mu_2(x_1) & \mu_2(x_2) & ... & \mu_2(x_k) \\ ... & ... & ... & ... \\ \mu_k(x_1) & \mu_k(x_2) & ... & \mu_k(x_k) \end{pmatrix}.$$

Решение такой системы не вызывает сложностей, хотя в общем случае она может быть и несовместной.

Несмотря на достаточно простой способ решения новой системы, к недостатку данного метода можно отнести необходимость искусственного ограничения мощностей множеств V_i и/или D_i, что может ухудшать качество принимаемых управленческих решений.

Способ 2. Использование метода наименьших квадратов.

Для этого необходимо дополнить систему (1) разными сочетаниями свойств ситуации и соответственно результатами экспертного опроса. При этом следует рассмотреть $b = min\ (k, r)$ различных линейно независимых сочетаний. Полученная система

$$\begin{pmatrix} zv_{11} & zv_{12} & ... & zv_{1k} \\ zv_{21} & zv_{22} & ... & zv_{2k} \\ ... & ... & ... & ... \\ zv_{b1} & zv_{b2} & ... & zv_{bk} \end{pmatrix}_i \cdot \begin{pmatrix} \alpha_{11} & \alpha_{12} & ... & \alpha_{1r} \\ \alpha_{21} & \alpha_{22} & ... & \alpha_{2r} \\ ... & ... & ... & ... \\ \alpha_{k1} & \alpha_{k2} & ... & \alpha_{kr} \end{pmatrix}_i = \begin{pmatrix} \mu_1(x_1) & \mu_1(x_2) & ... & \mu_1(x_r) \\ \mu_2(x_1) & \mu_2(x_2) & ... & \mu_2(x_r) \\ ... & ... & ... & ... \\ \mu_b(x_1) & \mu_b(x_2) & ... & \mu_b(x_r) \end{pmatrix}$$

переписывается в b систем вида

$$\begin{pmatrix} zv_{11} & zv_{12} & ... & zv_{1k} \\ zv_{21} & zv_{22} & ... & zv_{2k} \\ ... & ... & ... & ... \\ zv_{b1} & zv_{b2} & ... & zv_{bk} \end{pmatrix}_i \cdot \begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ ... \\ \alpha_{k1} \end{pmatrix}_i = \begin{pmatrix} \mu_1(x_1) \\ \mu_2(x_1) \\ ... \\ \mu_b(x_1) \end{pmatrix},$$

$$\begin{pmatrix} zv_{11} & zv_{12} & ... & zv_{1k} \\ zv_{21} & zv_{22} & ... & zv_{2k} \\ ... & ... & ... & ... \\ zv_{b1} & zv_{b2} & ... & zv_{bk} \end{pmatrix}_i \cdot \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ ... \\ \alpha_{k2} \end{pmatrix}_i = \begin{pmatrix} \mu_1(x_2) \\ \mu_2(x_2) \\ ... \\ \mu_b(x_2) \end{pmatrix} \text{ и т.д.}$$

Для каждой такой системы находят наилучшее решение $A^0=(\alpha_{ij}^0,..., \alpha_{kj}^0)$, для которого при значениях $\alpha_{1j} = \alpha_{1j}^0$, $\alpha_{2j} = \alpha_{2j}^0$, …, $\alpha_{kj} = \alpha_{kj}^0$ квадратичное отклонение

$$\left|M_j - [zv_i] \cdot A\right|^2 = \sum_{i=1}^{b} \left|\mu_i(x_j) - \sum_{l=1}^{k} zv_{ik}\alpha_{ki}\right|^2$$

достигает своего наименьшего значения. Поиск наилучшего решения может быть осуществлён с помощью псевдообратной матрицы, полученной методом Гревиля [3].

Использование второго способа, хоть и при значительных объёмах вычислений, позволяет определить значения искомых коэффициентов $[\alpha_{kr}]_i$, а соответственно и функцию F_i без необходимости ограничения исходных данных.

Рассмотрение различных ситуаций позволяет получить набор различных функций F_i. Таким образом, при возникновении кризисной ситуации правило принятия решения будет включать в себя следующие этапы:

1. Классификация ситуации, т.е. определение, к какой типовой ситуации s_i относится рассматриваемый случай.
2. Определение значений свойств zv_i рассматриваемой ситуации.
3. Выбор соответствующей функции F_i.
4. Расчёт значений функций принадлежности для действий из D_i.
5. Определение значений лингвистической переменной x.
6. Реализация действий, для которых необходимость использования очень сильная, сильная и средняя.

Заключение

Представленные в статье решения требуют для их использования в практической деятельности проведения значительной аналитической работы по определению функций экстраполяции и обучению сотрудников органов внутренних дел их применению. В то же время используемые методы решений основаны на уже имеющихся в информационных системах сведениях, т.е. требуют лишь их программной реализации в удобном для применения пользователями виде. Разработка соответствующего информационно-аналитического обеспечения деятельности органов внутренних дел в рамках модернизации правоохранительной системы является актуальной и востребованной задачей.

ЛИТЕРАТУРА

1. Филатов Н.В., Конюхов А.В. Разработка архитектуры информационной системы в рамках аппаратно-программного комплекса «Безопасный город» // Вестник Воронежского института МВД России. —2011. — №4. — С. 88—93.

2. Меньших В.В., Пьянков О.В., Самороковский А.Ф. Использование современных информационных технологий для обучения действиям в кризисных ситуациях // Вестник Воронежского института МВД России. — 2011. — №3. — С. 154—160.

3. Пьянков О.В., Самороковский А.Ф. Обработка экспертных оценок действий органов внутренних дел при возникновении чрезвычайных обстоятельств // Вестник Воронежского института МВД России. — 2009. — №2. — С. 131—135.

4. Обработка нечеткой информации в системах принятия решений / А.Н. Борисов [и др.]. — М.: Радио и связь,1989. — 304 с.

5. Орлов А.И. Прикладная статистика: учебник для вузов. — М.: Экзамен, 2004. — 656 с.

СВЕДЕНИЯ ОБ АВТОРАХ:

Пьянков Олег Викторович. Заместитель начальника кафедры инфокоммуникационных систем и технологий. Кандидат технических наук, доцент.
Воронежский институт МВД России.
E-mail: pyankovov@vimvd.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 262-33-85.

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.

Pyankov Oleg Victorovich. The deputy chief of chair of Infocommunication Systems and Technologies. Candidate of technical sciences, assistant professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. 8-904-210-34-19.

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.

Ключевые слова: принятие решений; экстраполяция; метод наименьших квадратов.

Key words: decision-making; extrapolation; the method of least squares.

УДК 517.9

В.В. Волхонский,
кандидат технических наук, доцент,
Санкт-Петербургский национальный
исследовательский университет
информационных технологий, механики
и оптики

ОПТИМИЗАЦИЯ СТРУКТУРЫ И АЛГОРИТМОВ РАБОТЫ КОМБИНИРОВАННЫХ СРЕДСТВ ОБНАРУЖЕНИЯ ПРОНИКНОВЕНИЯ НАРУШИТЕЛЯ

OPTIMIZATION OF STRUCTURE AND OPERATION ALGHORITHMS OF DUAL TECHNOLOGY INTRUSION DETECTORS

Выполнен анализ уязвимых мест комбинированных устройств обнаружения нарушителя. Предложено использовать разнесенные ортогональные комбинированные извещатели, позволяющие обеспечить высокую вероятность обнаружения и низкий уровень ложных тревог.

Analyzes of dual technology detectors vulnerability is accomplished. Mutually spaced orthogonal dual technology detectors are offered with high intrusion detection probability and low level of false alarm.

Введение

Вопросы обеспечения физической безопасности различных объектов, например, носителей и средств обработки информации, мест хранения материальных или культурных ценностей и т.п. объектов являются весьма важными. При разработке и анализе эффективности системы охранной сигнализации, обычно используемой для таких целей, одной из основных является задача достижения высокой вероятности обнаружения несанкционированного проникновения (НП). Особенно это существенно, если ставится задача охраны важных объектов, что объясняется возрастанием вероятности применения со стороны нарушителя методов и средств, снижающих возможность его обнаружения.

В работе [1] рассмотрены и проанализированы основные факторы, влияющие на средства обнаружения НП (т.е. на извещатели), в работе [2] — потенциальные воздействия на извещатели охранной сигнализации со стороны квалифицированного нарушителя и даны некоторые общие рекомендации по построению структуры средств обнаружения (СО) на объекте. Там же показано, что многорубежная охрана дает выигрыш в основном при обнаружении неподготовленного нарушителя. В работе [3] рассматриваются вопросы количественной оценки вероятности обнаружения при различных направлениях движения нарушителя, но только для одного типа устройств обнаружения — пассивного инфракрасного (ПИК) извещателя и без привязки к структуре СО на

объекте. В работе [4] проанализированы основные особенности использования СО с одним каналом обнаружения, совмещенных и двойной технологии (т.е. комбинированных) в рассматриваемых условиях.

Как и следовало ожидать, наилучшие результаты по достижению высокой вероятности обнаружения обеспечивают комбинированные извещатели охранной сигнализации, как наиболее эффективные с точки зрения соотношения вероятностей обнаружения и ложной тревоги. Но остается проблема недостаточной их защищенности от воздействий нарушителя — во всех случаях, как одиночных, так и совмещенных или комбинированных СО, есть способы воздействия, приводящие к существенному снижению вероятности обнаружения подготовленного или высококвалифицированного нарушителя. Следовательно, можно сделать вывод о целесообразности разработки и оптимизации более эффективных структур СО на объекте и алгоритмов принятия решения о проникновении.

Критерии оптимизации

Основными критериями оптимизации структуры и алгоритмов работы средств обнаружения несанкционированного проникновения для рассматриваемой задачи могут служить:

высокая вероятность обнаружения $P_{\text{об}}$;

низкая вероятность ложной тревоги $P_{\text{лт}}$;

защищенность извещателя, способность сохранять свои характеристики при тех или иных видах воздействий или приемов, применяемых нарушителем для преодоления системы сигнализации.

Первые два критерия достаточно активно используются на практике, но требования к реализации желаемых значений $P_{\text{об}}$ и $P_{\text{лт}}$ противоречивы, поскольку увеличение вероятности обнаружения связано с необходимостью повышения чувствительности, в свою очередь, приводящей к росту вероятности ложного срабатывания. А требование снижения вероятности ложного срабатывания ведет к необходимости снижения чувствительности с соответствующим уменьшением вероятности обнаружения НП. Как известно, основное решение, позволяющее реализовать компромисс между вероятностями обнаружения и ложной тревоги, достигается путем использования комбинированных устройств [1].

В общем случае вероятность обнаружения будет функцией нескольких основных параметров. К их числу, как наиболее часто используемых и наиболее эффективных, можно отнести, прежде всего, следующие:

эффективная отражающая/излучающая поверхность $E_{\text{эф}}$ нарушителя;

скорость v движения нарушителя;

направление движения, которое можно характеризовать углом φ относительно направления на извещатель.

Тогда вероятность обнаружения можно записать как функцию перечисленных выше параметров $P_{\text{об}}\left(E_{\text{эф}}, v, \varphi\right)$. Вероятность $P_{\text{лт}}$ зависит от выбора контролируемых обнаружителем параметров $\mathbf{O}^i$ объекта и наличия подобных по воздействию факторов $\mathbf{E}^j$ в окружающей среде [2]. Таким образом, в общем случае надо решать задачу оптимизации $P_{\text{об}}$ и $P_{\text{лт}}$ по определенному критерию Ψ, например минимаксному

$$\Psi\left\{\max\left[P_{\text{об}}(E_{\text{эф}}, v, \varphi)\right], \min\left[P_{\text{лт}}(\mathbf{O}^i, \mathbf{E}^j)\right]\right\}. \quad (1)$$

Использование этого критерия не исключает необходимости выполнения и критерия несовместности эффективных воздействий на СО [2]:

$$\bigcup_{n\in N} S_n^{j\text{эф}} \cap \bigcup_{l\in N} S_l^{k\text{эф}} = \varnothing,\ j,k \in K\ . \qquad (2)$$

При этом в общем виде совокупность эффективных воздействий $S_i^{j\text{вф}}$ включает в себя N возможных факторов воздействия $\mathbf{E}^j = [E_1^j, E_2^j, ..., E_N^j]$, определяющих окружающие условия; множество $\mathbf{B}^j = [B_1^j, B_2^j, ..., B_M^j]$ из M возможных пассивных способов воздействия B_n^j на j-е средство обнаружения и совокупность L активных способов воздействия $\mathbf{A}^j = [A_1^j, A_2^j, ..., A_L^j,]$ на j-е СО. Ограничимся случаем учета влияния первых двух факторов — окружающей среды $\mathbf{E}^j$ и пассивных воздействий нарушителя $\mathbf{B}^j$.

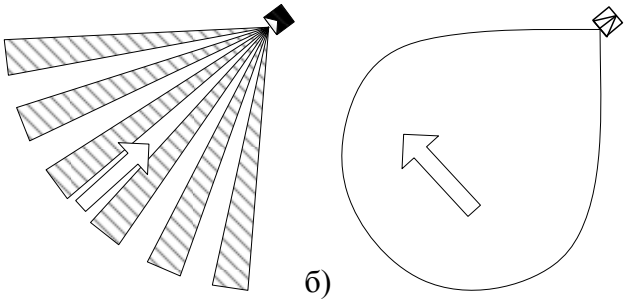
Выполнение критерия (2) требуется как при разработке самих извещателей, так и при формировании их структуры на объекте. Это достигается в современных комбинированных извещателях сочетанием радиоволнового (РВ) и пассивного инфракрасного (ПИК) обнаружителей и совместной обработкой по правилу «И».

Рассмотрим, прежде всего, такой наиболее доступный и эффективный способ воздействия нарушителя на один из каналов обнаружения, как выбор направления движения, при котором чувствительность одного из обнаружителей комбинированных СО минимальна. В этом случае можно считать $v = const$ и $E_{\text{эф}} = const$ и критерий (1) упрощается и принимает вид

$$\Psi\left\{\max\left[P_{\text{об}}(\ \varphi)\right], \min\left[P_{\text{лт}}(\mathbf{O}^i, \mathbf{E}^j)\right]\right\}\Big|_{v=const,\, E_{\text{эф}}=const}\ .$$

Анализ существующих структур

Как показано в [3], при использовании одиночного ПИК детектора умышленное перемещение нарушителя в радиальном направлении (рис. 1, а) может приводить к существенному уменьшению вероятности обнаружения. Учитывая принцип действия допплеровских радиоволновых и ультразвуковых извещателей [1], можно говорить об уменьшении вероятности обнаружения при тангенциальном направлении движения относительно них (рис. 1, б). Т.е. достаточно просто найти уязвимое место типичных типов СО и использовать его для преодоления системы охранной сигнализации.



а) б)

Рис. 1. Радиальное движение нарушителя относительно ПИК извещателя (а) и тангенциальное относительно РВ (б)

Для случая совмещенных СО при использовании многорубежной охраны (т.е. соответствующем алгоритму принятия решения «ИЛИ») в [2] показана необходимость выполнения следующих требований:

перекрытия зон обнаружения любых СО (рис. 2);

совмещения СО разного принципа действия в одном месте (рис. 2, а);

разнесения в смежные углы СО одного принципа действия (рис. 2, б, в).

Это соответствует структурам СО, изображенным на рис. 2, которые позволяют устранить часть уязвимостей структуры СО, имеющих место при неперекрывающихся зонах обнаружения, когда не выполняется условие (2).

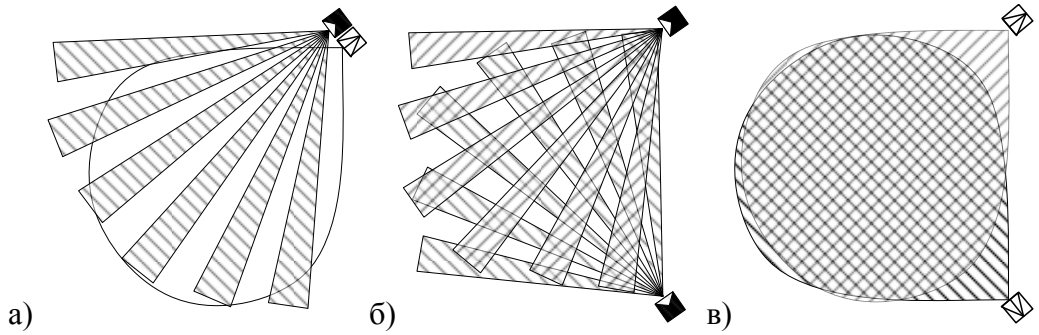


Рис. 2. Варианты организации контроля зоны при многорубежной охране с использованием одиночных обнаружителей

Такие решения, как показанные на рис. 2, позволяют повысить вероятность правильного обнаружения, поскольку во всех этих случаях есть обнаружитель, эффективный к тому или иному направлению движения. Однако при этом сохраняется сложность решения проблемы снижения уровня ложных тревог.

Как известно, необходимость применения комбинированных устройств обнаружения вызвана требованием достижения высокой вероятности обнаружения при сохранении низкого уровня ложных тревог. Это достигается использованием двух каналов обнаружения с совмещением их зон обнаружения (рис. 3) и принятием решения по алгоритму «И», что позволяет повысить чувствительность обоих каналов обнаружения и, следовательно, увеличить вероятность обнаружения.

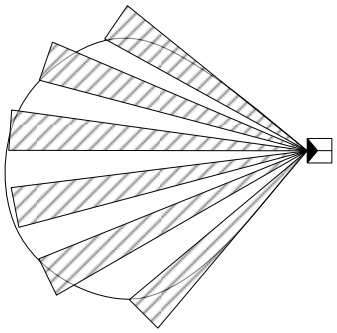


Рис. 3. Зоны обнаружения каналов комбинированного детектора

Рост вероятности ложной тревоги при этом компенсируется использованием алгоритма «И» и правильным выбором принципов действия каналов, основанном на приведенном выше критерии несовместности. Это будет частный случай выражения (2) с учетом только окружающих условий

$$\bigcup_{n\in N} E_n^j \cap \bigcup_{l\in N} E_l^k = \varnothing . \qquad (3)$$

Однако в рассматриваемом случае есть возможность воздействия нарушителя для снижения вероятности обнаружения только одного из каналов $P_{об1}$ или $P_{об2}$. И, вследствие использования алгоритма «И», вероятность обнаружения в целом $P_{об\Sigma}$ будет меньше наименьшей $P_{об\Sigma} = P_{об1} P_{об2}$. Т.е. у нарушителя имеется возможность эффективного снижения суммарной вероятности своего обнаружения.

Разнесенные ортогональные комбинированные детекторы

Рассмотрим возможности усовершенствования структур СО, показанных выше и позволяющих реализовать предложенный критерий оптимизации на основе комбинированных СО.

Разнесенный ортогональный детектор

Для решения задачи оптимизации можно предложить использовать пару одиночных РВ и ПИК обнаружителей, также работающих по алгоритму «И», но разнесенных в пространстве (установленные в разных местах) и развернутых относительно друг друга, а именно, расположенных в смежных углах помещения и развернутых на угол $\varphi=90^0$ относительно осей диаграмм направленности (рис. 4). В этом случае будет направление движения НП (радиальное для ПИК и тангенциальное для РВ), одинаково эффективно обнаруживаемое обоими каналами. Будем называть такую структуру разнесенным ортогональным детектором (РОД).

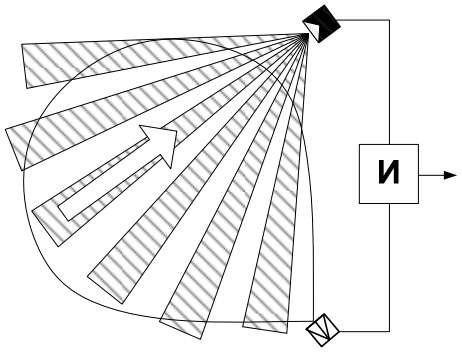


Рис. 4. Разнесенный ортогональный детектор

Но в этом случае будет направление радиальное для ПИК и тангенциальное для РВ обнаружителей (рис. 4), при движении нарушителя в котором вероятность обнаружения мала. Следовательно, будет иметь место уязвимость такой структуры СО. Однако это устройство можно эффективно использовать при наличии естественных ограничителей потенциального направления движения нарушителя или в случае известного наиболее вероятного направления движения.

Сдвоенные разнесенные ортогональные детекторы

Для устранения упомянутой выше уязвимости РОД можно предложить следующее решение. Снижения вероятности обнаружения при движении нарушителя в произвольном направлении можно избежать, используя два разнесенных ортогональных детектора с «зеркальной» структурой, то есть применяя структуру СО, состоящую из двух пар разнесенных ортогональных детекторов, рассмотренных выше и установленных, как показано на рис. 5 следующим образом.

Отдельные обнаружители первого РОД расположены в тех же смежных углах помещения, что и у другой пары обнаружителей второго РОД.

В одном углу устанавливаются отдельные обнаружители каждого РОД разного физического принципа действия.

Зоны обнаружения всех устройств перекрываются.

Алгоритм обработки сигналов пары обнаружителей каждого РОД использует правило «И».

Общее решение принимается по алгоритму «ИЛИ», т.е. для принятия решения о тревоге должен сработать хотя бы один из РОД.

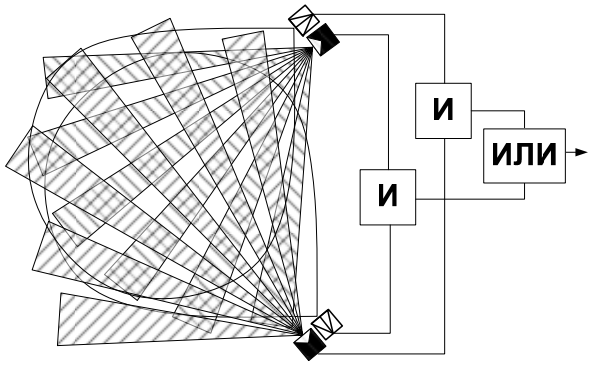


Рис. 5. Сдвоенные разнесенные ортогональные детекторы

При этом достигаются следующие преимущества.

Сохраняются достоинства традиционных комбинированных извещателей, а именно возможность использовать высокую чувствительность каналов обнаружения без опасения роста вероятности ложной тревоги.

Практически исключается рассматриваемая уязвимость традиционных комбинированных СО, связанная с возможностью снижения вероятности обнаружения путем выбора направления движения нарушителем.

Таким образом, в предложенной структуре решается поставленная выше задача оптимизации структуры СО с учетом используемых критериев.

Заключение

Сформулируем полученные результаты.

1. Выполнен анализ существующих структур традиционных средств обнаружения в условиях профессиональных способов проникновения на охраняемый объект и проанализированы структуры СО на основе использования пар одиночных извещателей с принятием решения по правилу «ИЛИ».

2. Предложены структура и алгоритм работы разнесенного ортогонального комбинированного детектора, позволяющего достичь высокой вероятности обнаружения нарушителя, двигающегося в одном направлении, при низкой вероятности ложной тревоги. Предлагаемый РОД состоит из одной пары отдельных разнесенных в пространстве обнаружителей с разным физическим принципом действия с совмещенными зонами обнаружения, оси которых перпендикулярны, и с обработкой сигналов по правилу «И».

3. Предложены структура и алгоритм работы сдвоенного разнесенного ортогонального комбинированного обнаружителя, позволяющего достичь высокой вероятности обнаружения нарушителя, двигающегося в произвольном направлении, при низкой

вероятности ложной тревоги, который состоит из двух пар отдельных разнесенных ортогональных детекторов с зеркальным расположением каналов обнаружения с совместной обработкой их сигналов по правилу «ИЛИ».

ЛИТЕРАТУРА

1. Волхонский В.В. Извещатели охранной сигнализации. — Изд. 4-е доп. и перераб. — СПб.: Экополис и культура. — 2004. — 272 с.

2. Волхонский В.В., Крупнов А.Г. Особенности разработки структуры средств обнаружения угроз охраняемому объекту // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. — 2011. — № 4(74). — С. 131—136.

3. Волхонский В.В., Воробьев П.А. Методика оценки вероятности обнаружения несанкционированного проникновения оптикоэлектронным извещателем // Научно-технический вестник информационных технологий, механики и оптики. — 2012. — №1(77). — С. 120—123.

4. Волхонский В.В. К вопросу повышения вероятности обнаружения несанкционированного проникновения на охраняемый объект // Вестник Воронежского института МВД России. — 2011. — №4. — С. 35—44.

СВЕДЕНИЯ ОБ АВТОРЕ:

Волхонский Владимир Владимирович. Профессор кафедры твердотельной оптоэлектроники. Кандидат технических наук, доцент.

Федеральное государственное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

E-mail: volkhonski@mail.ru

Россия, 197101, Санкт-Петербург, Кронверкский проспект, 49. Тел.7 (921) 964 97 10.

Volkhonskiy Vladimir Vladimirovich. Professor of the chair of Solid State Optoelectronics. Candidate of sciences (technical), assistant professor.

Saint-Petersburg National Research University of Information Technology, Mechanics and Optics.

Work address: 197101, Russia, Saint-Petersburg, Kronverkskiy prospect, 49. Tel. +7 (921) 964 97 10.

Ключевые слова: система безопасности; средства обнаружения; комбинированный извещатель.

Key words: security system; intrusion detectors; dual technology detector.

УДК 654.924

О.С. Авсентьев,
доктор технических наук, профессор

Н.И. Гомова

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МЕХАНИЗМОВ ПЕРЕХВАТА ИНФОРМАЦИИ ПО ПАРАМЕТРИЧЕСКИМ КАНАЛАМ И ПРОТИВОДЕЙСТВИЯ ЕЕ УТЕЧКЕ

MATHEMATICAL MODEL OF THE MECHANISM INTERSEPTION ON PARAMETRIC CHANNELS AND ITS COUNTER RELEASE

Предлагается методический подход к формированию показателя для оценки эффективности противодействия угрозам утечки информации по параметрическим каналам как вероятностной характеристики достаточности выполняемых функций. Рассмотрены варианты представления показателя для оценки эффективности противодействия угрозам утечки информации по параметрическим каналам для различных композиционных вариантов структурирования целевой функции моделируемого процесса.

The methodical approach is used to form the indicators of evaluation of the effective resistance to leaked through the parametric channels. The effectiveness of resistance in its term is the characteristics of the sufficiency of response measures to the threat appeared as a result of illegal informational interception. The options of the indicators of evaluation of the effective resistance to leaked through the parametric channels for different compositional variations, the options of the structuring of the objective function of modelling process are considered.

В соответствии с концептуальными положениями теории моделирования сложных систем процесс моделирования, в общем случае, должен осуществляться в три этапа:

Первый этап — обобщенное описание объекта моделирования в терминах качественного представления наиболее значимых для объекта связей.

Второй этап — первичная формализация объекта моделирования путем структуризации его обобщенного описания.

Третий этап — сопоставление детализированному описанию объекта моделирования соответствующих математических моделей, отвечающих целям моделирования [1], либо признаков взаимодействия объекта моделирования с внешней средой в терминах его структурного (детализированного) представления [2].

На первом и втором этапах рассматриваемого процесса моделирования с целью анализа исследуемых механизмов утечки информации по параметрическим каналам в интересах оценки эффективности противодействия утечке используются методы структурного синтеза [3] и технологии построения описательных моделей, как средства первичной формализации объекта исследования, позволяющие понизить сложность его описания, но не дающие возможность использовать их в качестве средств математического моделирования вследствие сложности представления в реальном времени логики функционирования объекта, его аналитического описания и оценки показателей качества функционирования.

В настоящей работе предлагается методический подход к исследованию механизмов перехвата информации по параметрическим каналам и противодействия утечке математическими методами на третьем этапе рассматриваемого процесса моделирования.

Представление противоправных действий по перехвату информации по параметрическим каналам утечки в виде обобщенной функциональной модели позволяет сформировать математическое представление подобного рода действий и создать предпосылки для количественной оценки угроз утечки информации по параметрическим каналам.

С этой целью определим показатель A достаточности выполняемых функций по реагированию на угрозы утечки информации по параметрическим каналам, возникающим в результате противоправных действий по ее перехвату.

Принимая во внимание, что наибольшее влияние на такого рода характеристику оказывает соотношение между временными характеристиками выполняемых операций при реализации угроз и способов технической защиты информации, в качестве основы для конструирования соответствующего показателя условимся использовать время $\tau_{(p)}$ реализации функций, выполняемых при реагировании на угрозы утечки информации. Меры по противодействию угрозе считаются достаточными, если время $\tau_{(p)}$ меньше требуемого $\tau_{(m)}$, обусловленного спецификой угрозы, т.е. при выполнении неравенства:

$$\tau_{(p)} < \tau_{(m)}. \qquad (1)$$

В общем случае обе входящие в неравенство (1) величины являются случайными, поэтому его выполнение является случайным событием. Вероятность этого события $P(\tau_{(p)} < \tau_{(m)})$ довольно полно характеризует достаточность выполняемых функций по реагированию на угрозы утечки информации по параметрическим каналам, что позволяет использовать ее в качестве показателя A для оценки эффективности противодействия угрозам, т.е.

$$A = P(\tau_{(p)} < \tau_{(m)}). \qquad (2)$$

С учетом того, что угрозы утечки информации по параметрическим каналам и противодействие этим угрозам являются противоположными событиями, показатель R степени угрозы перехвата информации определим по формуле:

$$R = 1 - A = 1 - P(\tau_{(p)} < \tau_{(m)}) = P(\tau_{(p)} \geq \tau_{(m)}). \qquad (3)$$

Принимая во внимание, что целевую функцию $\Phi^{(n)}$ «Противодействие угрозам утечки информации по параметрическим каналам» структурно составляют две функции (первый уровень ее декомпозиции):

$\phi_1^{(n1)}$ — «Реагирование на угрозы перехвата информации по параметрическим каналам утечки вне контролируемой зоны»;

$\phi_2^{(n1)}$ — «Реагирование на угрозы перехвата информации по параметрическим каналам утечки в контролируемой зоне»,

обозначим через a_n достаточность выполняемых функций по реагированию на угрозы

утечки информации по параметрическим каналам при реализации противоправной функции $\phi_i^{(n1)}$, $i = 1, 2$.

Тогда выражение (3) можно записать в виде:

$$R = (1 - a_1)\cdot(1 - a_2),$$

где a_1 — достаточность выполняемых функций по реагированию на угрозы перехвата информации по параметрическим каналам утечки вне контролируемой зоны при реализации противоправной функции $\phi_1^{(n1)}$, т.е. $a_1 = a_1(\phi_1^{(n1)})$;

a_2 — достаточность выполняемых функций по реагированию на угрозы перехвата информации по параметрическим каналам утечки в контролируемой зоне при реализации противоправной функции $\phi_2^{(n1)}$, т.е. $a_2 = a_2(\phi_2^{(n1)})$.

При этом r_i определяется по формуле:

$$r_i = 1 - a_i = 1 - P(\tau_{(p)i} < \tau_{(m)i}), \quad (4)$$

в которой $\tau_{(p)i}$ — время реализации функции $\phi_i^{(n1)}$, i =1, 2;

$\tau_{(m)i}$ — требуемое значение времени реализации функции $\phi_i^{(n1)}$.

Исходя из того, что каждую из функций $\phi_i^{(n1)}$, i =1, 2 структурно составляют функции второго уровня декомпозиции целевой функции, входящую в выражение (4) величину времени $\tau_{(p)i}$ можно представить в виде:

$$\tau_{(p)i} = \sum_{j=1}^{J_i} \circ \tau_{(p)i,j} ,$$

где $\tau_{(p)\,i,j}$ — характеристика времени реализации функции $\phi_{i,j}^{(n2)}$, составляющей функцию $\phi_i^{(n1)}$;

J_i — количество функций, составляющих функцию $\phi_i^{(n1)}$;

$\sum_{j=1}^{J_i} \circ$ — операция, означающая композицию J_i случайных величин [1].

Случайный характер времен $\tau_{(m)i}$ и $\tau_{(p)i}$ приводит к следующему представлению выражения для показателя r_i степени угрозы перехвата информации по параметрическим каналам утечки вне контролируемой зоны (i=1) и в ее пределах (i=2):

$$r_i = P\left(\tau_{(p)i} > \tau_{(m)i}\right) = \int_0^{\overline{\tau}_{(p)i}} f_{(m)i}(w)\,dw , \quad (5)$$

где $f_{(m)i}$ — функция плотности вероятности случайной величины $\tau_{(m)i}$;

$\overline{\tau}_{(p)i}$ — среднее значение времени $\tau_{(p)i}$.

Практика решения задач оценки эффективности реализации различного рода информационных процессов, связанных с комбинированием методов имитационного и аналитического моделирования позволила получить ряд выражений [1] показателей вида (5).

В основу этих аналитических выражений положена обобщенная интегральная формула вида:

$$P(x < y) = \int_0^{\overline{x}} f(y)\,dy , \quad (6)$$

в которой $\overline{x}$ — среднее значение случайной величины x; $f(y)$ — плотность распределения случайной величины y.

Следует отметить, что композиционные составляющие величины x могут реализовываться либо параллельно, либо последовательно (соответственно, функции

$\phi_{i,j}^{(n2)}$, $\phi_{i,k}^{(n2)}$, j, $k = 1, 2, \ldots, J_i, j \neq k$ могут выполняться либо параллельно, либо последовательно).

В первом случае величина x определяется согласно выражению [4]:

$$\bar{x} = \sum_{l=1}^{L} p_{(l)} \cdot x_{(l)}, \tag{7}$$

в котором $p_{(l)}$ — вероятность реализации l-го состояния ($\sum_{l=1}^{L} p_{(l)} = 1$);

$x_{(l)}$ — характеристика l-го состояния;

L — число состояний.

Во втором случае величина $\bar{x}$ определяется согласно выражениям [1]:

$$\bar{x} = x_{(1)} \circ x_{(2)} = \int_{x_{(1)\ min}}^{\infty} u \int_{x_{(2)\ min}}^{\infty} f_{(1)}(u - u_{\text{I}})\, f_{(2)}(u_1)\, du_{\text{I}}\, du, \tag{8}$$

если величина $\bar{x}$ представляет собой композицию двух случайных величин;

$$\bar{x} = M\left(x_{(1)} \circ x_{(2)} \circ x_{(3)}\right) = \int_0^{\infty}\int_0^{u}\int_0^{u_{\text{II}}} u \cdot f_1(u_1) \cdot f_2(u_{\text{II}} - u_{\text{I}}) f_3(u - u_{\text{II}})\, du_{\text{I}}\, du_{\text{II}} du, \tag{9}$$

если величина $\bar{x}$ представляет собой композицию трех случайных величин;

$$\bar{x} = M\left(x_{(1)} \circ x_{(2)} \circ x_{(3)} \circ x_{(4)}\right) = \int_0^{\infty}\int_0^{u}\int_0^{u_{\text{I}}}\int_0^{u_{\text{III}}} u \cdot f_1(u_1) \cdot f_2(u_{\text{II}} - u_{\text{I}}) \cdot f_3(u_{\text{III}} - u_{\text{II}}) \cdot f_4(u - u_{\text{III}})\, du_{\text{I}}\, du_{\text{II}} du_{\text{III}} du, \tag{10}$$

если величина $\bar{x}$ представляет собой композицию четырех случайных величин;

$$\bar{x} = M\left(\sum_{l=1}^{L} \bar{x}_{(l)}\right), \tag{11}$$

если величина $\bar{x}$ представляет собой композицию более четырех случайных величин ($L > 4$).

В выражениях (8) — (10) $f_{(1)}, f_{(2)}, f_{(3)}$ и $f_{(4)}$ — плотности распределений случайных величин $x_{(1)}$, $x_{(2)}$, $x_{(3)}$ и $x_{(4)}$, соответственно, в выражении (8) $x_{(1)\ \min}$ и $x_{(2)\ \min}$ — минимальные значения случайных величин $x_{(1)}$ и $x_{(2)}$, соответственно; в выражении (11) $\bar{x}_{(l)}$ — среднее значение величины $x_{(l)}$.

Вместе с тем имеется ряд ограничений на применение выражений вида (5) и (6) для оценки угроз утечки информации по параметрическим каналам.

Ограничение 1. Случайные величины $x_{(1)}$, $x_{(2)}$, $x_{(3)}$ и $x_{(4)}$ могут аппроксимироваться равномерным, экспоненциальным или нормальным законом распределения. Ниже приводятся выражения для плотности распределения этих величин (для простоты индексы не приводятся):

для равномерного закона:

$$f(x) = \begin{cases} 0, \text{ при } x > x_{\max}, x < x_{\min} \\ \dfrac{1}{x_{\max} - x_{\min}}, \text{ при } x_{\min} < x < x_{\max}, \end{cases}$$

где $x_{\min}$ и $x_{\max}$ минимальное и максимальное значение x, соответственно;

для экспоненциального закона:

$$f(x)=\begin{cases}0, \text{ при } x < x_{\min};\\ \dfrac{1}{\bar{x}}\exp\left(-\dfrac{x-x_{\min}}{\bar{x}}\right), \text{при } x \ge x_{\min},\end{cases}$$

где $\bar{x}$ — среднее значение случайной величины x;

$x_{\min}$ — минимальное значение x;

для нормального закона:

$$f(x)=\begin{cases}0, \text{ при } x < x_{\min};\\ \dfrac{1}{\sigma\sqrt{2\pi}}\exp\left(-\dfrac{(x-\bar{x})^2}{2\sigma^2}\right), \text{при } x \ge x_{\min},\end{cases}$$

где $\bar{x}$ — среднее значение случайной величины x;

σ — среднеквадратичное отклонение x;

$x_{\min}$ — минимальное значение x.

В [1] представлены выражения для определения $\bar{x}$ в условиях такой аппроксимации.

Ограничение 2. Случайная величина y аппроксимируется экспоненциальным законом распределения, что приводит к следующему решению интеграла (6):

$$P(x < y)=1-\exp\left(-\frac{\bar{x}-y_{\min}}{\bar{y}}\right). \quad (12)$$

С учетом (1) и (12) выражение для оценки показателя A эффективности противодействия угрозам утечки информации по параметрическим каналам, в соответствии с (2), будет иметь вид:

$$P(\tau_{(p)} < \tau_{(m)})=1-\exp\left(-\frac{\bar{\tau}_{(p)}-\bar{\tau}_{(m)\min}}{\bar{\tau}_{(m)}}\right). \quad (13)$$

Аналогичные рассуждения относятся и к нижним уровням композиционной структуры противоправных действий.

Ограничение 1 можно считать несущественным, так как равномерный, экспоненциальный или нормальный законы распределения случайных величин являются классообразующими.

Ограничение 2 несущественно ввиду того, что в соответствии с положениями теории исследования операций поток заявок на обслуживание системой, в том числе и воздействий угроз утечки информации по техническим каналам, с достаточной степенью адекватности аппроксимируется пуассоновским распределением [5]. При этом длительность воздействий подчиняется экспоненциальному закону распределения.

Аналогичные рассуждения применимы к функциям других уровней декомпозиции целевой функции «Противодействие угрозам утечки информации по параметрическим каналам».

В связи с тем что составляющие основу сформированного показателя для оценки эффективности противодействия утечке информации по параметрическим каналам временные параметры имеют объективную природу, обусловленную объективными условиями совершения противоправных действий с одной стороны и соответствующих действий по защите информации с другой стороны, такой показатель может служить для количественной оценки степени угроз утечки информации по параметрическим каналам.

ЛИТЕРАТУРА

1. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / под научн. ред. С.В. Скрыля. — Воронеж: Воронежский институт МВД России, 2010. — 211 с.

2. Криминалистическая идентификация признаков несанкционированного доступа к защищенным компьютерным системам / С.В. Скрыль и [др.] // Безопасность информационных технологий. — М.: МИФИ, 2006. — № 2 (50). — С. 67—70.

3. Скрыль С.В., Шелупанов А.А. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105. — М.: Машиностроение, 2008. — 138 с.

4. Теория вероятностей. — М.: Изд-во физико-математической литературы, 1958. — 464 с.

5. Вентцель Е.С. Исследование операций. — М.: Советское радио, 1972. — 552 с.

СВЕДЕНИЯ ОБ АВТОРАХ:

Авсентьев Олег Сергеевич. Профессор кафедры информационной безопасности. Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: osaos@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 262-33-76.

Гомова Наталья Ивановна. Адъюнкт кафедры информационной безопасности.
Воронежский институт МВД России.
E-mail: gomova.nata2008@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 262-33-76.

Avsentjev Oleg Sergeevitch. Professor of Information Security chair. Doctor of technical sciences, professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 262-33-76.

Gomova Natalya Ivanovna. The post-graduate cadet of Information Security chair.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 262-33-76.

Ключевые слова: математическая модель; показатель для оценки эффективности противодействия утечке информации по параметрическим каналам; угроза утечки информации; время реализации функций.

Key words: mathematical model; the indicator of evaluation of the effective resistance to leaked through the parametric channels; the threat of leaked; the time period of realization of the functions.

УДК 621.3