Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

# ИНТЕРЭКСПО ГЕО-СИБИРЬ

XV Международный научный конгресс

Сборник материалов в 9 т.

Т. 9
Национальная конференция

## «НАУКА. ОБОРОНА. БЕЗОПАСНОСТЬ-2019»

Новосибирск
СГУГиТ
2019

УДК 614.18
С26

Ответственные за выпуск:

Доктор экономических наук, член-корреспондент РА РАН,
заместитель генерального директора по развитию
АО «Научно-исследовательский институт электронных приборов», г. Новосибирск
*В. Г. Эдвабник*

Начальник отдела Управления ФСТЭК России по СФО, г. Новосибирск
*В. В. Селифанов*

Доктор технических наук, доцент,
заведующий кафедрой специальных устройств, инноватики
и метрологии СГУГиТ, г. Новосибирск
*В. С. Айрапетян*

Доктор экономических наук, директор Института оптики
и оптических технологий СГУГиТ, г. Новосибирск
*А. В. Шабурова*

С26 Интерэкспо ГЕО-Сибирь. XV Междунар. науч. конгр., 24–26 апреля 2019 г., Новосибирск [Текст] : сб. материалов в 9 т. Т. 9 : Нац. конф. «Наука. Оборона. Безопасность-2019». – Новосибирск : СГУГиТ, 2019. – 148 с. – ISSN 2618-981X

DOI: 10.33764/2618-981X-2019-9

В сборнике опубликованы материалы XV Международного научного конгресса «Интерэкспо ГЕО-Сибирь», представленные на Национальной конференции «Наука. Оборона. Безопасность-2019».

Печатается по решению редакционно-издательского совета СГУГиТ

Материалы публикуются в авторской редакции

УДК 614.18



---

Сборник включен в систему РИНЦ.

УДК 004.632
DOI: 10.33764/2618-981X-2019-9-3-14

# МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ В УСЛОВИЯХ ВНЕШНИХ ПРЕДНАМЕРЕННЫХ РАЗРУШАЮЩИХ ВОЗДЕЙСТВИЙ

***Сергей Николаевич Новиков***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, зав. кафедрой информационной безопасности, e-mail: snovikov@ngs.ru

В работе предложена математическая модель функционирования мультисервисной сети связи в условиях внешних деструктивных воздействий, учитывающая: структуру сети; пропускные способности трактов передачи сообщений; вероятностно-временные параметры (интенсивность поступления, плотность распределения) входящего в сеть информационного потока пакетов сообщений различных приложений; метод маршрутизации.

**Ключевые слова:** мультисервисная сеть связи, внешние деструктивные воздействия.

# MATHEMATICAL MODEL OF FUNCTIONING OF MODERN TELECOMMUNICATION SYSTEMS IN THE CONDITIONS OF EXTERNAL DELIBERATE DESTRUCTIVE INFLUENCES

***Sergei N. Novikov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Head of Department of Information Security, e-mail: snovikov@ngs.ru

The paper proposes a mathematical model of the functioning of a multiservice communication network under external destructive influences, taking into account: network structure, capacity of message transmission paths; probabilistic-temporal parameters (intensity of income, density of distribution) of information packet of messages of various applications entering the network; routing method.

**Key words:** multiservice communication network, external destructive influences.

## Концепция логической структуры математической модели

На рис. 1 представлена концепция математической модели.

Исходными данными являются: структура мультисервисной сети связи (МСС) с множеством узлов коммутации (УК) и линий связи (ЛС); метод маршрутизации; входящий в МСС асинхронный поток пакетов различных приложений, доступных пользователям; степень тяготения УИ к УП для передачи пакетов сообщений $\varepsilon$-го приложения МСС; внешнее деструктивное воздействие на элементы МСС.

Каждое приложение МСС характеризуется вероятностно-временными характеристиками (скорость передачи, время задержки, временной джиттер, вероятность ошибочного приема на символ, пакет, сообщение и многие другие). Неподдержание данных параметров (со стороны МСС) приводит к отказу в обслуживании данных приложений, следовательно, к снижению QoS МСС.

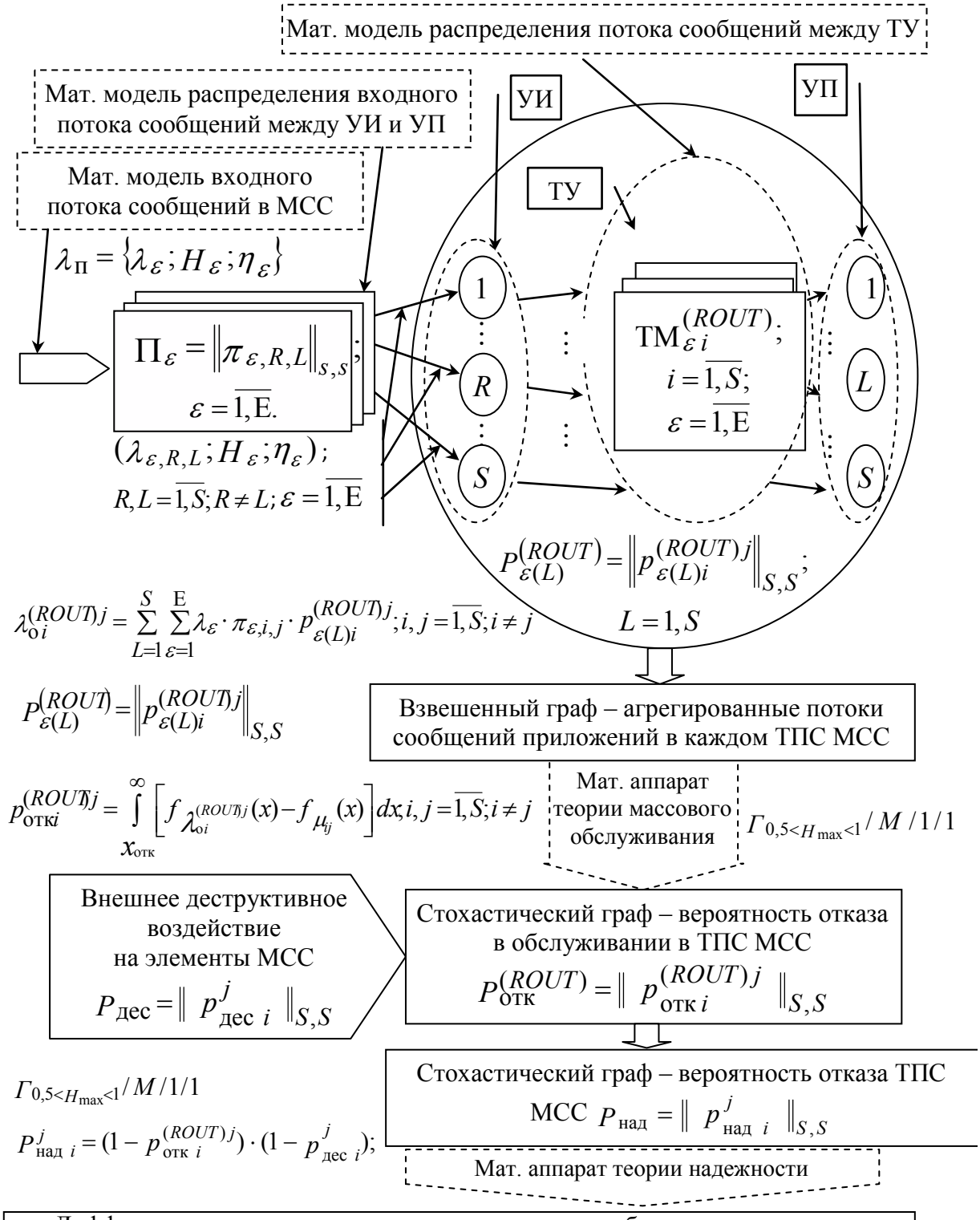



Рис. 1. Концепция математической модели маршрутизации в МСС

В этой связи обобщающим параметром качества функционирования МСС примем вероятность отказа в обслуживании выбранных пользователями приложений.

Таким образом, критериями функционирования МСС примем: вероятность отказа в обслуживании в целом по МСС – интегральная оценка; вероятность отказа в обслуживании между каждой парой УИ и УП в МСС – дифференциальная оценка.

Порядок определения искомых вероятностей следующий. Входящий в МСС информационный поток пакетов сообщений $\varepsilon$-го приложения в соответствии со степенью тяготения УИ к УП дезагрегируется на отдельные потоки, которые поступают в соответствующие УИ для последующей передачи в соответствующие УП.

В каждом тракте передачи сообщений (ТПС) формируются виртуальные каналы (ВК) и виртуальные тракты (ВТ) передачи сообщений. Это означает что, на канальном уровне МВОС в трактах передачи сообщений формируется асинхронный поток пакетов ($\Pi_i$) (рис. 2).

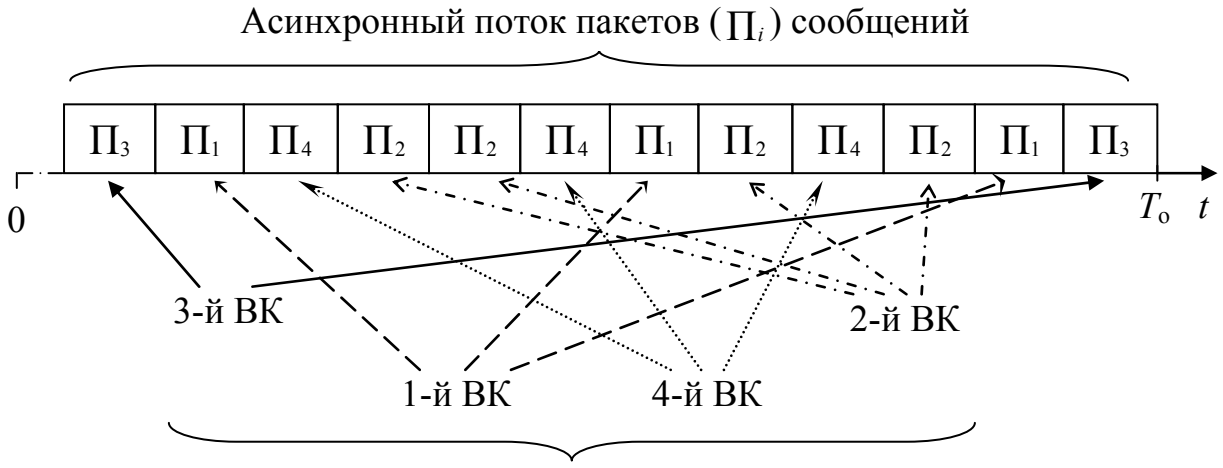



Рис. 2. Пример формирования ВК в одном ВТ за время наблюдения $T_o$

Подчиняясь заранее определенной процедуре маршрутизации, потоки сообщений различных приложений в каждом УК (УИ и транзитных узлах (ТУ)) распределяются по всем трактам передачи сообщений МСС. Далее, агрегируя распределенные потоки сообщений в каждом тракте, определяется суммарный поток каждого тракта передачи сообщений МСС. Учитывая, что ТПС обладает определенной пропускной способностью, появляется возможность применить аппарат теории массового обслуживания. А именно, определить вероятность отказа в обслуживании агрегируемого потока сообщений в каждом тракте МСС. В результате получаем стохастический граф, ребрам которого присвоены вероятности отказа обслуживания приложений МСС.

Внешнее деструктивное воздействие (ВДВ) реализуется в заранее заданных вероятностях отказа ТПС мультисервисной сети связи. Если допустить, что вероятности отказа обслуживания приложений МСС в каждом ТПС и вероятности отказа самих ТПС (по причине ВДВ) являются независимыми событиями, то данные вероятности перемножаются. В результате получаем новый стохастический граф, ребрам которого присвоены вероятности их отказа.

Далее, используя математический аппарат теории надежностей, имеется возможность расчета искомых значений.

Таким образом, изменяя: основные параметры МСС (структуру, пропускные способности ТПС); вероятностно-временные параметры (интенсивность поступления, плотность распределения) входящего в МСС информационного потока пакетов сообщений; параметры ВДВ на МСС, имеется возможность провести анализ функционирования МСС в условиях ВДВ.

## Формальное описание исходных данных математической модели

1. Структуру МСС представим в виде неориентированного графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\}; i = \overline{1, S}$, соответствующих УК; ребер $M_S = \{m_{ij}\}; i, j = \overline{1, S}; i \neq j$, соответствующих ТПС.

Каждый ТПС характеризуется пропускной способностью $\mu_{ij}; i, j = \overline{1, S}; i \neq j$ – наибольшим количеством пакетов, передаваемых за единицу времени. В качестве допущения примем, что длительность обслуживания пакетов сообщений поступающего асинхронного потока данных в ТПС между $a_i$ и $a_j$ УК $i, j = \overline{1, S}; i \neq j$ (рис. 2) подчиняется экспоненциальному закону с параметром:

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1, S}; i \neq j. \qquad (1)$$

2. Метод маршрутизации $ROUT = \{ROUT_{\text{тм}} \uparrow ROUT_{\text{сс}}\}$ зададим процедурой выбора исходящих ТПС на множестве $S$ пошаговых таблиц маршрутизации для $\varepsilon$-го приложения:

$$P_{\varepsilon}^{(j)} = \left\| p_{\varepsilon,i,\nu}^{(j)} \right\|_{(S-1),\chi_j} = \left( \overline{p_{\varepsilon,1}^{(j)}}, \ldots, \overline{p_{\varepsilon,i}^{(j)}}, \ldots, \overline{p_{\varepsilon,j-1}^{(j)}}, \overline{p_{\varepsilon,j+1}^{(j)}}, \ldots, \overline{p_{\varepsilon,S}^{(j)}} \right), \varepsilon = \overline{1, \mathrm{E}}, \qquad (2)$$

где $\overline{P_{\varepsilon,i}^{(j)}} = (p_{\varepsilon,i,\nu}^{(j)}); \sum_{\nu=1}^{\chi_j} p_{\varepsilon,i,\nu}^{(j)} = 1; \nu = \overline{1, \chi_j}; i, j = \overline{1, S};$ $\chi_j$ – степень $a_j$-го УК.

Матрицей (2) задается план распределения информации для $\varepsilon$-го приложения.

Элементы вектора $\overline{p_{\varepsilon,i}^{(j)}}$ определяют вероятность того, что для $\varepsilon$-го приложения на этапе поиска маршрута к $a_j$-му УП в $a_i$-м транзитном УК, начиная с УИ, будет выбрана ν-я исходящая ЛС.

3. Входящий в МСС информационный поток характеризуется интенсивностью поступления пакетов сообщений $\varepsilon$-го приложения в $a_R$-й УИ для последующей передачи в $a_L$-й УП:

$$(\lambda_{\varepsilon,R,L}; H_\varepsilon; \eta_\varepsilon), \tag{3}$$

где $H_\varepsilon$ – параметр Херста $\varepsilon$-го приложения; $\eta_\varepsilon$ – средняя длина пакетов сообщений $\varepsilon$-го приложения.

Плотность распределения вероятностей последовательности промежутков между вызовами поступления пакетов сообщений $\varepsilon$-го приложения в $a_R$-й УИ для последующей передачи в $a_L$-й УП определим выражением:

$$f(x) = \begin{cases} \dfrac{\lambda_{\varepsilon,R,L}^{H_\varepsilon} \cdot x^{H_\varepsilon - 1} \cdot e^{-\lambda_{\varepsilon,R,L} \cdot x}}{\Gamma(H_\varepsilon)}; R, L = \overline{1,S}; R \neq L; \varepsilon = \overline{1,\mathrm{E}}; x \geq 0; \\ 0, \qquad\qquad x < 0, \end{cases} \tag{4}$$

где $\Gamma(H_\varepsilon) = \int\limits_0^\infty x^{H_\varepsilon - 1} \cdot e^{-x} dx$ – гамма-функция.

В работе [2] получены результаты, утверждающие, что при агрегировании самоподобных потоков результирующий поток будет тоже самоподобным с параметрами:

$$H = \max_i (H_i); i = \overline{1,N}; \lambda = \sum_{i=1}^{N} \lambda_i. \tag{5}$$

Следовательно, интенсивность потока данных $\varepsilon$-го приложения, поступающего в МСС, составит:

$$\lambda_\varepsilon = \sum_{R,L=1}^{S} \lambda_{\varepsilon,R,L}.$$

4. Вероятность поступления потока данных $\varepsilon$-го приложения в $a_R$-й УИ для его последующей передачи $a_L$-му УП определяется матрицей тяготений:

$$\Pi_\varepsilon = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S},$$

где $0 \le \pi_{\varepsilon,R,L} = \dfrac{\lambda_{\varepsilon,R,L}}{\lambda_{\varepsilon}} \le 1; \sum\limits_{R,N=1}^{S} \pi_{\varepsilon,R,L} = 1; \varepsilon = \overline{1,\mathrm{E}}.$

5. ВДВ на элементы МСС представим в виде матрицы:

$$P_{\text{дес}} = \| \; p^{j}_{\text{дес } i} \; \|_{S,S},$$

где $p^{j}_{\text{дес } i}$ – вероятность выхода из строя ребра $m_{i,j}$ исходного графа $G[A_S, M_S]$, описывающего структуру мультисервисной сети связи.

Критериями оценки функционирования МСС примем:

$$\{\hat{P}_{\text{отк}}; \hat{p}^{(R,L)}_{\text{отк}}\} = f\{G[A_S, M_S]; \Pi_{\varepsilon}; \lambda_{\varepsilon}; H_{\varepsilon}; \mu; ROUT; P_{\text{дес}}\}; R, L = \overline{1,L}; R \ne L; \varepsilon = \overline{1,\mathrm{E}}, \quad (6)$$

где $\hat{P}_{\text{отк}}$ – вероятность отказа в обслуживании в целом по сети – интегральная оценка; $\hat{P}^{(R,L)}_{\text{отк}}; R, T = \overline{1,L}; R \ne L$ – вероятность отказа в обслуживании между УИ ($a_R$) и УП ($a_L$) – дифференциальная оценка.

### *Разработка математической модели распределения потока сообщений между транзитными узлами МСС*

Отождествим вершины графа (сети) $G[A_S, M_S]$ с состояниями конечной цепи Маркова. Из набора векторов (2) для метода маршрутизации $ROUT$ и $\varepsilon$-го приложения МСС при поиске $a_L$-го УК можно получить матрицу переходных вероятностей [1]:

$$P^{(ROUT)}_{\varepsilon(L)} = \left\| p^{(ROUT)j}_{\varepsilon(L)i} \right\|_{S,S} i, j = \overline{1,S},$$

где $p^{(ROUT)j}_{\varepsilon(L)i}; i, j = \overline{1,S}$ – вероятность перехода из состояния $a_i$ в $a_j$ конечной цепи Маркова для метода маршрутизации $ROUT$ и $\varepsilon$-го приложения МСС при поиске $a_L$-го УК. Причем состояние $a_L$, соответствующее $a_L$-му УК (УП), определим поглощающим, т.е.

$$P^{(ROUT)L}_{\varepsilon(L)L} = 1.$$

Матрица переходных вероятностей, описывающая вероятности переходов для поиска $a_L$-го УК при методе маршрутизации $ROUT$ и $\varepsilon$-м приложении МСС, будет иметь вид:

$$\left|\begin{array}{c|cccccc} & 1 & \cdots & L & \cdots & (S-1) & S \\ 1 & 0 & \cdots & p^{(ROUT)L}_{\varepsilon(L)\ 1} & \cdots & p^{(ROUT)S-1}_{\varepsilon(L)\ 1} & p^{(ROUT)S}_{\varepsilon(L)\ 1} \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots \\ L & 0 & \cdots & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots \\ S-1 & p^{(ROUT)1}_{\varepsilon(L)\ S-1} & \cdots & p^{(ROUT)L}_{\varepsilon(L)\ S-1} & \cdots & 0 & p^{(ROUT)S}_{\varepsilon(L)\ S-1} \\ S & p^{(ROUT)1}_{\varepsilon(L)\ S} & \cdots & p^{(ROUT)L}_{\varepsilon(L)\ S} & \cdots & p^{(ROUT)S-1}_{\varepsilon(L)\ S} & 0 \end{array}\right|. \quad (7)$$

Интенсивность потоков в ТПС $m_{ij}; i, j = \overline{1,S}; i \neq j$ при поиске $a_L$-го УК, методе маршрутизации $ROUT$ и $\varepsilon$-м приложении МСС составит:

$$\lambda^{(ROUT)j}_{\varepsilon(L)i} = p^{(ROUT)j}_{\varepsilon(L)i} \cdot \lambda_{\varepsilon,i,L}; i, j = \overline{1,S}; i \neq j,$$

причем из свойства конечных цепей Маркова имеем:

$$\lambda_{\varepsilon,i,L} = \sum_{j=1}^{S} \lambda^{(ROUT)j}_{\varepsilon(L)i}; i, j = \overline{1,S}; i \neq j.$$

Общие интенсивности потоков всех $\varepsilon = \overline{1,\mathrm{E}}.$ приложений в ТПС $m_{i,j}; i, j = \overline{1,S}; i \neq j$ при заданном методе маршрутизации $ROUT$ определятся из системы уравнений:

$$\lambda^{(ROUT)j}_{\mathrm{o}\,i} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} \lambda^{(ROUT)j}_{\varepsilon(L)i} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} p^{(ROUT)j}_{\varepsilon(L)i} \cdot \lambda_{\varepsilon,i,L}; i, j = \overline{1,S}; i \neq j$$

или

$$\lambda^{(ROUT)j}_{\mathrm{o}\,i} = \sum_{L=1}^{S}\sum_{\varepsilon=1}^{\mathrm{E}} \lambda_{\varepsilon} \cdot \pi_{\varepsilon,i,j} \cdot p^{(ROUT)j}_{\varepsilon(L)i}; i, j = \overline{1,S}; i \neq j, \quad (8)$$

где $\lambda_{\varepsilon}$ – интенсивность поступления потока данных $\varepsilon$-го приложения в МСС;

$\pi_{\varepsilon,i,j}$ – элемент матрицы тяготений $\Pi_{\varepsilon}$; $p^{(ROUT)j}_{\varepsilon(L)\,i}$ – элемент матрицы переходных вероятностей $P^{(ROUT)}_{\varepsilon(L)}$.

В результате получаем взвешенный граф, каждому ребру которого присвоены агрегированные потоки сообщений всех E приложений:

$$\lambda^{(ROUT)}_{\mathrm{o}} = \left\| \lambda^{(ROUT)j}_{\mathrm{o}\,i} \right\|_{S,S}. \quad (9)$$

Так как входящие информационные потоки в мультисервисную сеть связи подчиняются гамма-распределению с параметрами $(\lambda_{\varepsilon,R,L}; H_\varepsilon; \eta_\varepsilon)$, то с учетом (5) можно утверждать, что и агрегированные потоки сообщений (9) тоже подчиняются гамма-распределению. При этом параметр Херста выбирается максимальным из всех $H_\varepsilon; \varepsilon = \overline{1, \mathrm{E}}$.

Принятое ограничение (1) (экспоненциальный закон распределения длительности обслуживания пакетов сообщений) с параметром

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1, S}; i \neq j,$$

позволяет воспользоваться математическим аппаратом теории массового обслуживания для расчета вероятности отказа в обслуживании агрегированных потоков сообщений (9) в ТПС между $a_i$ и $a_j$ УК.

Каждое ребро графа (9) в обозначениях Кендалла представим как $\Gamma_{0,5<H_{\max}<1} / M / 1 / 1$. Здесь $\Gamma_{0,5<H_{\max}<1}$ – обозначение гамма-распределения (с параметром Херста $0{,}5 < H_{\max} < 1$ и интенсивностью $\lambda_{\text{о}i}^{(ROUT)j}; i, j = \overline{1, S}; i \neq j$) случайной длины интервала между соседними требованиями входного потока; $M$ – экспоненциальная функция распределения случайного времени обслуживания агрегированных потоков сообщений с параметром:

$$w_{ij} = \frac{1}{\mu_{ij}}; i, j = \overline{1, S}; i \neq j.$$

Из графического представления плотности распределения случайной длины интервала между соседними требованиями входного потока ($f_{\lambda_{\text{о}i}^{(ROUT)j}}(x)$) и плотности распределения случайного времени обслуживания агрегированных потоков сообщений ($f_{\mu_{ij}}(x)$) (рис. 3) определим общее выражение вероятности отказа в обслуживании агрегированных потоков сообщений (9) в ТПС между $a_i$ и $a_j$ УК:

$$p_{\text{отк}\,i}^{(ROUT)j} = \int_{x_{\text{отк}}}^{\infty} \left[ f_{\lambda_{\text{о}i}^{(ROUT)j}}(x) - f_{\mu_{ij}}(x) \right] dx; i, j = \overline{1, S}; i \neq j. \qquad (10)$$

Окончательно получим:

$$p_{\text{отк}\,i}^{(ROUT)j} = \int_{x_{\text{отк}}}^{\infty} \left[ \frac{\lambda_{\text{о}i}^{(ROUT)} H_{\max} j \cdot x^{H_{\max}-1} \cdot e^{-\lambda_{\text{о}i}^{(ROUT)j \cdot x}}}{\int_0^{\infty} x^{H_{\max}-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1, S}; i \neq j. \qquad (11)$$

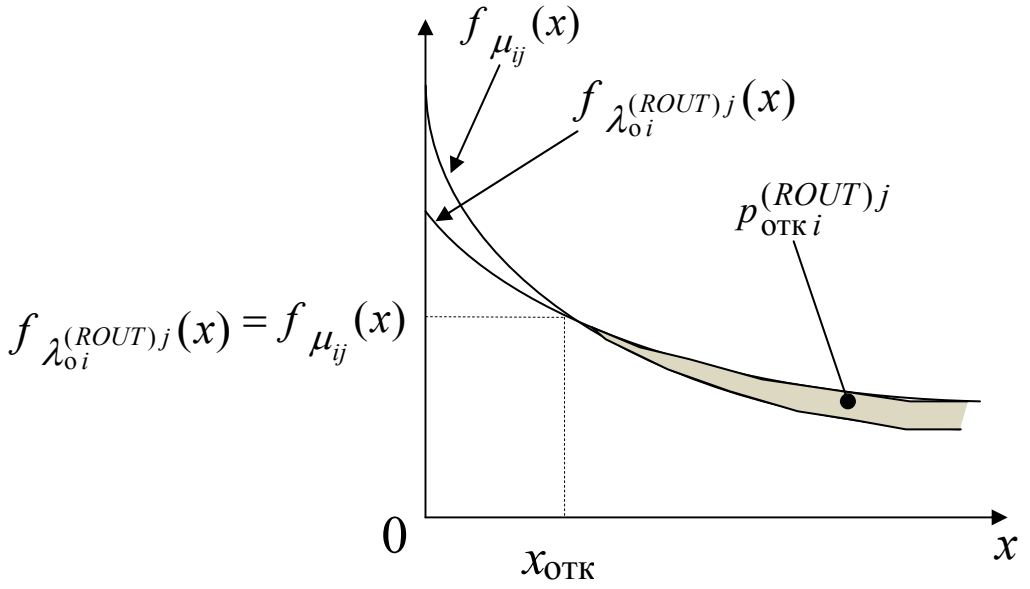



Рис. 3. Графическое определение общего выражения вероятности отказа в обслуживании агрегированных потоков сообщений в ТПС

Для практических исследований воспользуемся результатом работы [3], в которой искомая вероятность отказа в обслуживании получена для случая $\Gamma_{0,5}/M/1/N$:

$$p = \frac{\left(1 - \frac{\rho}{4} - \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right)}{1 - \left(\frac{\rho}{4} + \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right)^{N+1}} \left(\frac{\rho}{4} + \sqrt{\frac{\rho^2}{16} + \frac{\rho}{2}}\right)^{N},$$

где $\rho = \frac{\lambda}{\mu}$; $\lambda$ – интенсивность поступления заявок на входе системы массового обслуживания (СМО); $\mu$ – производительность обслуживающей линии СМО.

Таким образом, вероятность отказа в обслуживании агрегированных потоков сообщений в ТПС между $a_i$ и $a_j$ УК будем определять следующим образом:

$$p_{\text{отк}\,i}^{(ROUT)j} = \frac{\left(1 - \frac{\rho_i^{(ROUT)j}}{4} - \sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16} + \frac{\rho_i^{(ROUT)j}}{2}}\right)}{1 - \left(\frac{\rho_i^{(ROUT)j\ 2}}{4} + \sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16} + \frac{\rho_i^{(ROUT)j}}{2}}\right)^2} \times$$

$$\times\left(\frac{\rho_i^{(ROUT)J}}{4}+\sqrt{\frac{\rho_i^{(ROUT)j\ 2}}{16}+\frac{\rho_i^{(ROUT)j}}{2}}\right);i,j=\overline{1,S};i\neq j.$$

В результате получим стохастический граф, ребрам которого присвоены вероятности отказа в обслуживании в каждом ТПС для всех $\varepsilon=\overline{1,\mathrm{E}}.$ приложений МСС:

$$P_{\text{отк}}^{(ROUT)}=\|\ p_{\text{отк}\ i}^{(ROUT)j}\ \|_{S,S}. \tag{12}$$

Допустим, что внешнее деструктивное воздействие на элементы МСС и вероятности событий (12) являются независимыми. Тогда вероятности надежности ТПС МСС определим следующим образом:

$$P_{\text{над}\ i}^{j}=(1-p_{\text{отк}\ i}^{(ROUT)j})\cdot(1-p_{\text{дес}\ i}^{j});i,j=\overline{1,S};i\neq j. \tag{13}$$

В результате имеем стохастический граф, ребрам которого присвоены вероятности надежности всех ТПС МСС:

$$P_{\text{над}}=\|\ p_{\text{над}\ i}^{j}\ \|_{S,S}. \tag{14}$$

Далее, используя математический аппарат теории надежности [4], появляется возможность определить искомые значения (6). Для этого воспользуемся методом полного перебора оценки структурной надежности телекоммуникационной системы.

Пронумеруем элементы множества $M=\{m_{ij}\};i,j=\overline{1,S};i\neq j$ числами натурального ряда $M=\{m_{ij}\}=\{m_{\upsilon}\};i,j=\overline{1,S};i\neq j;\varphi=\overline{1,\kappa}.$ Каждое ребро анализируемого графа может находиться в двух состояниях:

$$\begin{cases}\sigma_\varphi=1\ \ (m_{ij}\ \text{исправно})\ \text{с вероятностью}\ p_\varphi=p_{\text{над}\,i}^{j};i,j=\overline{1,S};i\neq j;\varphi=\overline{1,\kappa};\\ \sigma_\varphi=0\ \ (m_{ij}\ \text{вышло из строя})\ \text{с вероятностью}\ q_\varphi=1-p_\varphi.\end{cases}$$

В этом случае анализируемый граф может находиться в одном из $k=\overline{1,2^\kappa}$ состояний. Вероятность каждого из возможных состояний графа определяется:

$$p_k=\prod_{\varphi=1}^{\kappa}p_\varphi^{\sigma_\nu}\cdot q_\varphi^{1-\sigma_\varphi};k=\overline{1,2^\kappa}.$$

Введем переменные:

$$Q_o^{(k)} = \begin{cases} 1, \text{если граф, находясь в } k \text{ - м состояни, связен;} \\ 0, \text{ в противном случае;} \end{cases}$$

$$Q_{ij}^{(k)} = \begin{cases} 1, \text{если граф, находясь в } k \text{ - м состоянии,} \\ \quad \text{обеспечивает связность вершин } a_i \text{ и } a_j; \\ 0, \text{в противном случае.} \end{cases}$$

В результате функционал (6) определяется выражениями:

$$\hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot \Big( \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi} \Big); R, L = \overline{1, S}; \qquad (15)$$

$$\hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi}. \qquad (16)$$

Таким образом, методика математического моделирования функционирования МСС состоит в решении следующей системы уравнений:

$$\begin{cases} P_{\varepsilon(L)}^{(ROUT)} = \left\| P_{\varepsilon(L)i}^{(ROUT)j} \right\|_{S,S} i, j = \overline{1, S}; \\ \lambda_{\text{o}\,i}^{(ROUT)j} = \sum_{L=1}^{S} \sum_{\varepsilon=1}^{\text{E}} \lambda_\varepsilon \cdot \pi_{\varepsilon,i,j} \cdot p_{\varepsilon(L)i}^{(ROUT)j}; i, j = \overline{1, S}; i \neq j; \\ p_{\text{отк}\ i}^{(ROUT)j} = \int_{x_{\text{отк}}}^{\infty} \left[ \dfrac{\lambda_{\text{o}\,i}^{(ROUT)} H_{\max} {}^{j} \cdot x^{H_{\max}-1} \cdot e^{-\lambda_{\text{o}\,i}^{(ROUT)j \cdot x}}}{\int_0^\infty x^{H_{\max}-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1, S}; i \neq j; \\ P_{\text{над}\ i}^{j} = (1 - p_{\text{отк}\ i}^{(ROUT)j}) \cdot (1 - p_{\text{дес}\ i}^{j}); i, j = \overline{1, S; i \neq j}; \\ \hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_{RL}^{(k)} \cdot \Big( \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi} \Big); R, L = \overline{1, S}; \\ \hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^\kappa} Q_o^{(k)} \prod_{\varphi=1}^{\kappa} p_\varphi^{\sigma_\varphi} \cdot q_\varphi^{1-\sigma_\varphi}. \end{cases} \qquad (17)$$

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новиков, С. Н. Методы маршрутизации на цифровых широкополосных сетях связи: учеб. пособие по специальности 200900. – Сети связи и системы коммутации / С. Н. Новиков. – Новосибирск: СибГУТИ. – Ч. 1.– 2001. – 83 с.

2. Агеев, Д. В. Методика определения параметров потоков на разных участках мультисервисной телекоммуникационной сети с учетом самоподобия [Электронный ресурс] / Д. В. Агеев, А. А. Игнатенко, А. Н. Копылев // Проблемы телекоммуникаций : электрон. науч. специализир. изд.–журнал. – 2011. – № 5. – С. 16–37. – Режим доступа: http://pt.journal.kh.ua.

3. Пономарев, Д. Ю. Исследование моделей потоков вызовов [Электронный ресурс] / Д. Ю. Пономарев. – Режим доступа: http://www.nsc.ru/ws/YM2004/ 8509/index.html.

4. Новиков, С. Н. Методы оценки структурной надежности телекоммуникационных систем : учеб. пособие : метод. комплекс / С. Н. Новиков, Е. В. Сафонов. – Новосибирск, 2004. – 44 с.

УДК 004.491
DOI: 10.33764/2618-981X-2019-9-15-18

# ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ БОРЬБЫ С НИМ

***Тимофей Владимирович Таржанов***
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

***Вадим Евгеньевич Кудряшов***
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, обучающийся

***Диана Георгиевна Макарова***
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: kaf.ib@ssga.ru

В статье рассматривается существующее вредоносное программное обеспечение. Для изучения особенностей построения вредоносного программного обеспечения были проанализированы самые распространенные компьютерные вирусы. Разработана программа по захвату нажатий клавиатуры средствами языка Python 3.7, а также реализована функция отправки на почту захваченных данных.

**Ключевые слова:** вирус, вредоносное программное обеспечение, средства защиты информации, антивирусное программное обеспечение.

# DELETRIOUS SOFTWARE AND METHODS FOR COMBATING IT

***Timofey V. Tarzhanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

***Vadim E. Kudryashov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student

***Diana G. Makarova***
Siberian State University of Geosystems and Technologies,10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: kaf.ib@ssga.ru

The article discusses existing malware. To study the features of building deletrious software, the most common computer viruses were analyzed. A program for capturing keystrokes by means of the Python 3.7 language was developed, and a function for sending captured data to mail was implemented.

**Key words:** virus, malware, information security tools, antivirus software.

Компьютерный вирус – вид вредоносного программного обеспечения, способный внедряться в код других исполняемых программ, системные области памяти, загрузочные секторы, а также распространять свои копии, используя различные каналы связи.

Первые вирусные эпидемии относятся к 1986–1989 годам: Brain (вызвал крупнейшую эпидемию), Jerusalem (уничтожал программы при их запуске), червь Морриса (свыше 6200 компьютеров было заражено, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах). Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса), «троянские кони» (AIDS), полиморфные вирусы (Chameleon), стелс-вирусы (Frodo, Whale) [1–3].

В настоящее время принято разделять следующие категории вирусов:

– по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

– файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят зараженный файл, «спутники» идут отдельным файлом.

– по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);

– по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

– по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

– по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

В настоящее время наибольшее распространение получило следующее вредоносное программное обеспечение:

– вирус – программное обеспечение, которое дублирует себя множество раз и внедряет эти копии в другие программы и файлы;

– червь – то же, что и вирусы, но в отличие от них, у червей единицей заражения являются не файлы и документы, а компьютеры (иногда, сетевые устройства);

– логическая бомба – специфический вид вредоносных программ, который проявляет себя только при определенных действиях или событиях (наступление дат, открытие каких-либо файлов и прочее), а остальную часть времени бездействует;

– троян, или троянский конь – программное обеспечение, которое может не только выдавать себя за полезную программу, но и в реальности предоставлять полезные функции, в качестве прикрытия для деструктивных действий;

– клавиатурный шпион – особый вид трояна, который записывает все нажатия кнопок клавиатуры и/или действия мышки на вашем компьютере;

– руткит – скрытый тип вредоносного программного обеспечения, который выполняется на уровне ядра операционной системы. Основной опасностью руткитов является то, что, внедряясь на уровень ядра системы, руткиты могут выполнять любые действия и с легкостью обходить любые системы защиты, ведь для своего скрытия им достаточно отказать в доступе средствам безопасности.

Для отработки методики антивирусного программного обеспечения была смоделирована работа клавиатурного шпиона (кейлоггера).

Кейлоггер – программное обеспечение, регистрирующее различные действия пользователя, а именно, нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д. Кейлоггеры оказались самым распространенным способом кражи конфиденциальной информации, передвинув фишинг на второе место, и действуют все более избирательно: отслеживая веб-страницы, к которым обращается пользователь, они записывают нажатия клавиш только при заходе на сайты, интересующие злоумышленников [4].

Предложенный кейлоггер реализуется одним скриптом, в котором описаны следующие функции:

– функция addStartup() добавляет созданный кейлоггер в реестр, он будет запускаться автоматически при загрузке ОС;

– функция Hide() маскирует работу вируса, предотвращая появление командной строки (консоли);

– функция Mail_it() отвечает за отправку захваченной информации по почте;

– функция OnKeyboardEvent() отвечает за считывание нажатых клавиш и запись этой информации в текстовый файл.

Алгоритм работы предложенного кейлоггера следующий: пользователь запускает кейлоггер; программа перехватывает и записывает в текстовый файл нажатую клавишу, окно, в котором она была нажата, дату и время нажатия; затем происходит отправка захваченной информации на почту.

В работе кейлоггера возможны следующие варианты маскировки:

– с помощью утилиты pyinstaller создается exe-файл имеющегося скрипта. Создается его ярлык на рабочем столе рабочей станции, изменяется иконка и название, например на Skype. При запуске ярлыка ничего не открывается, но скрипт исполняется (в диспетчере задач процесс стал фоновым);

– из созданного exe-файла создается sfx-архив с помощью WinRAR. При открытии архива скрипт выполняется (в диспетчере задач процесс поменял название);

– через текстовый редактор создается bat-файл, который открывает одновременно браузер и exe-файл. Затем создается ярлык, прописав в объекте путь до имеющегося bat-файла (в диспетчере задач процесс скрыт);

– exe-файл маскируется под файл word, excel, или powerpoint с помощью утилиты backdoorppt. Этот вариант лучше остальных, так как он остается не-

замеченным антивирусным программным обеспечением, а в диспетчере задач процесс неотличим от исполнения процесса файлом word.

Наиболее актуальными методами защиты от кейлоггеров являются:

– использование одноразовых паролей;

– двухфакторная аутентификация;

– использование систем проактивной защиты, предназначенных для обнаружения программных кейлоггеров;

– использование виртуальных клавиатур.

Очевидно, что вредоносное программное обеспечение может быть использовано для кражи персональной информации и шпионажа. Компании, работающие в сфере компьютерной безопасности, фиксируют рост числа вредоносных программ, имеющих функциональность кейлоггера. В настоящее время кейлоггеры, наряду с фишингом и методами социальной инженерии, являются одним из главных методов электронного мошенничества. Все чаще в кейлоггеры добавляют rootkit-технологии, которые скрывают работу кейлоггера так, чтобы она не была видна ни пользователю, ни антивирусному программному обеспечению. Обнаружить и обезвредить такие кейлоггеры можно только с использованием специально разработанных средств защиты [5].

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. – М. : ДМК Пресс, 2013. – 656 с. – ISBN 978-5-94074-885-4. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/63192.

2. Монаппа, К. А. Анализ вредоносных программ / К. А. Монаппа ; перевод с английского Д. А. Беликова. – М. : ДМК Пресс, 2019. – 452 с. – ISBN 978-5-97060-700-8. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/123709.

3. Нестеров С. А. Основы информационной безопасности : учеб. пособие. – 5-е изд., стер. – Санкт-Петербург : Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/114688.

4. Жернаков, С.В. Система обнаружения вредоносных программ в операционной системе ANDROID / С.В. Жернаков, Г.Н. Гаврилов // Вестник Уфимского государственного авиационного технического университета. – 2016. – № 2. – С. 117-122. – ISSN 1992-6502. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/journal/issue/301803.

5. Keyloggers: How they work and how to detect them (Part 1) 2007. URL: https://securelist.com/analysis/publications/36138/keyloggers how they work and how to detect them part 1/.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-19-24

# ПРЕИМУЩЕСТВА МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

***Анастасия Сергеевна Голдобина***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, кафедра информационной безопасности, тел. (923)220-80-89,e-mail: nastya-gold09@mail.ru

***Игорь Николаевич Карманов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

***Полина Александровна Звягинцева***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Статья представляет значимость моделирования при внедрении разработанной системы на предприятие, помогая избежать существенных экономических потерь, и обеспечивая защиту информации при работе средств обнаружения вторжений, в информационных системах.

**Ключевые слова:** модель процессов управления, показатели эффективности, эффективности смоделированных процессов.

# ADVANTAGES OF SECURITY MANAGEMENT PROCESS MODELING OF STATE INFORMATION SYSTEMS

***Anastasia S. Goldobina***
Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630108, Russia, Student, Department of Information Security, phone: (923)220-80-89, e-mail: nastya-gold09@mail.ru

***Igor N. Karmanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Phisics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

***Polina A. Zviagintceva***
Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone:(383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

The article demonstrates the importance of modeling in the implementation of the developed system at the enterprise, helping to avoid significant economic losses, and providing protection of

information during the work of intrusion detection in information systems built with using optical equipment.

**Key words**: management processes model, efficiency indicators, efficiency of simulated processes.

Государственные информационные системы (ГИС) все чаще строятся на базе автоматизированных систем. Актуальность защиты информации в них обусловлена существенными изменениями в законодательстве Российской Федерации. ФСТЭК России рекомендует использовать моделирование процессов управления защитой информации в качестве предпроектного обследования для выявления недочетов до ввода ГИС в эксплуатацию.

Целью работы является обоснование проведения оценки эффективности для модели процессов управления защитой информации ГИС с использованием имитационной модели [1–3].

Существует три вида программ для имитационного моделирования:

– инструментарий имитационного моделирования, основанного на потоковых диаграммах;

– инструментарий динамического моделирования;

– инструментарий дискретно-событийного имитационного моделирования.

Для создания модели системы управления защитой информации необходимы функции последнего вида программ, которые позволяют пользователю выполнять наблюдение за движением в системе потоковых объектов, т.к. эти инструменты дают возможность моделировать потоки объектов. Наиболее распространенными системами имитационного моделирования являются следующие программы: AnyLogic, Arena, Simulink.

В работе было проанализировано 2 существующих способа построения модели. Первый способ управления параметрами объекта состоит в создании пропорциональных входного и выходного параметров в системе. При изменении выходного параметра система выдаст ошибку. Также устанавливаются пороговые сигналы системы, определяющие значения положительной и отрицательной величины отклонения от номинальной величины выходного параметра системы. Второй способ удаленного управления аппаратурой состоит в формировании на ПУ команд в виде управляющих сигналов и их передачи по линиям связи устройству приема команд и адресной выдачи управляющих сигналов.

В анализируемых работах были выявлены недостатки, снижающие функциональные возможности трехуровневого управления группами программных средств при использовании технического решения как в качестве способа, так и в качестве процессов трехуровневого управления программными средствами различного назначения.

Перечисленные отличительные признаки, позволяют расширить функциональные возможности системы трехуровневого алгоритма управления подсистемой обнаружения вторжений. Это реализуется за счет обеспечения выполнения функций управления в отделе мониторинга и безопасности и доопределе-

ния данных об объектах воздействия на пунктах управления АРМ в трехуровневой системе управления путем опроса системы, измерения состояния системы, удаленного измерения состояния системы, вычисления запущенных процессов и выбора объектов по характеристикам.

Трехуровневую модель процессов управления, возможно построить двумя способами:

– решение аналитической задачи;
– моделирование AnyLogic.

Для приема и обработки событий безопасности в защищаемой ГИС необходимо трехуровневое моделирование процессов управления системой защиты информации с использованием программного обеспечения AnyLogic для более точных расчетов.

Для построения имитационной модели процессов управления формализуются задачи под объект, что подразумевает описание процесса управления системой защиты информации с учетом приказа ФСТЭК России №17 на трех уровнях:

– третий – отдел мониторинга и безопасности;
– второй – сервера, на которых собранные данные автоматизируются;
– первый – автоматизированной рабочее место (далее – АРМ).

Формальная запись действия ${}^{j}D_i$ алгоритма означает i-е действие на j-м уровне моделирования. Алгоритм процессов управления выглядит следующим образом:

${}^{3}D_1$ – моделирование процесса создания команд на сбор данных об имеющихся в организации группах программных средств, объектах воздействия, условиях обстановки для управления системой защиты информации через пункт управления отдела мониторинга и безопасности;

${}^{3}D_2$ – моделирование процесса о ранжируемых данных для обнаружения и идентификации инцидентов об объектах воздействия для передачи в отдел мониторинга и безопасности;

${}^{3}D_3$ – моделирование процесса передачи данных об объектах, назначенных для осуществления управления средствами защиты информации, из пункта управления отдела мониторинга и безопасности на пункт управления сервера;

${}^{2}D_4$ – моделирование процесса приема данных об объектах, имеющихся в организации и назначенных для осуществления обнаружения и идентификации инцидентов, из пункта управления отдела мониторинга и безопасности на пункт управления сервера;

${}^{2}D_5$ – моделирование процесса проанализированных данных для регистрации и анализа событий безопасности между имеющимися в организации группами программных средств, объектах воздействия и условиях обстановки на полноту;

${}^{2}D_6$ – моделирование процесса распределения объектов воздействия для управления изменениями базовой конфигурации путем осуществления доопределения данных между пунктом управления сервера и пунктом управления АРМ, имеющимися в организации;

$^{2}D_{7}$ – моделирование процесса распределения каждого объекта воздействия для управления изменениями базовой конфигурации системы путем доопределения данных об объектах, имеющихся в организации, на два сервера, на одном из которых будет осуществляться непосредственное измерение состояния системы на пункт управления АРМ, а на другом – удаленное измерение состояния системы на пункт управления АРМ;

$^{2}D_{8}$ – моделирование процесса определения состояния системы для регистрации и анализа событий безопасности на пункт управления сервера;

$^{2}D_{9}$ – моделирование процесса измерения состояния системы для обнаружения и идентификации инцидентов на пункт управления сервера;

$^{2}D_{10}$ – моделирование процесса передачи значений состояния системы, предназначенных для одного или нескольких других серверов для управления изменениями базовой конфигурации системы одной группы программных средств, имеющихся в организации, в качестве удаленно измеренных;

$^{2}D_{11}$ – моделирование процесса приема удаленно измеренных значений состояния системы для обнаружения и идентификации инцидентов объектов воздействия, на другом пункте управления сервера, имеющемся в организации;

$^{2}D_{12}$ – моделирование процесса вычисления запущенных характеристик для контроля за событиями безопасности и действиями на пункт управления сервером;

$^{2}D_{13}$ – моделирование процесса выбора объектов по характеристикам для управления средствами защиты информации на пункт управления сервера;

$^{2}D_{14}$ – моделирование процесса доопределения данных о выделенной части объектов воздействия на пункт управления сервера. Одновременно с первым процессом происходит моделирование процесса формирования команды на доопределение данных о программных средствах, объектах воздействия и условиях обстановки, для управления изменениями базовой конфигурации системы, имеющейся в организации;

$^{2}D_{15}$ – моделирование процесса передачи команды на доопределение данных с пункта управления сервера на пункт управления АРМ, входящих в состав одной группы программных средств организации для управления средствами защиты информации;

$^{1}D_{16}$ – моделирование процесса формирования базы данных программных средств, объектов воздействия и условий обстановки, на пункт управления АРМ для регистрации и анализа событий в системе, имеющейся в организации;

$^{1}D_{17}$ – моделирование процесса определения состояния системы для регистрации и анализа событий на пункте управления АРМ;

$^{1}D_{18}$ – моделирование процесса измерения состояния системы для обнаружения и идентификации инцидентов на пункт управления АРМ;

$^{1}D_{19}$ – моделирование процесса передачи значений состояния системы, предназначенного для одного или нескольких других пунктов управления АРМ одной группы в качестве удаленно измеренных систем, на эти пункты управления АРМ для управления средствами защиты информации;

$^{1}D_{20}$ – моделирование процесса приема удаленно измеренных на другом пункте управления АРМ значений состояния системы объектов воздействия, для управления изменениями базовой конфигурации системы, имеющейся в организации;

$^{1}D_{21}$ – моделирование процесса вычисления запущенных процессов на пункте управления АРМ для контроля за событиями безопасности, имеющимися в организации;

$^{1}D_{22}$ – моделирование процесса выбора объектов по характеристикам на пункте управления АРМ для управления изменениями базовой конфигурации системы;

$^{1}D_{23}$ – моделирование процесса передачи данных на пункт управления сервера о программных средствах, объектах воздействия и условиях обстановки, для управления средствами защиты информации, имеющихся в организации;

$^{2}D_{24}$ – моделирование процесса сбора доопределенных данных на пункт управления сервера о состоянии программных средств группы, объектах воздействия и условиях обстановки, для регистрации и анализа событий системы, имеющейся в организации;

$^{2}D_{25}$ – моделирование процесса идентификации объектов воздействия на пункт управления сервера для обнаружения и идентификации системы;

$^{2}D_{26}$ – моделирование процесса классификации объектов воздействия на пункт управления сервера для контроля за событиями безопасности;

$^{2}D_{27}$ – моделирование процесса формирования списка объектов воздействия в соответствии с полученными значениями их приоритетов для управления изменениями базовой конфигурации системы;

$^{2}D_{28}$ – моделирование процесса оценки эффективности осуществления воздействия на внесенные в список приоритетных объектов воздействия штатными программными средствами, для контроля за событиями безопасности;

$^{2}D_{29}$ – моделирование процесса формирования списка программных средств, значения эффективности которых оказались достаточными для осуществления воздействия на объекты из сформированного списка для управления изменениями базовой конфигурации системы;

$^{2}D_{30}$ – моделирование процесса формирования команд управления в виде управляющих сигналов для управления изменениями базовой конфигурации;

$^{2}D_{31}$ – моделирование процесса передачи по каналам связи для обнаружения и идентификации инцидентов.

Система управления решает задачи управления, поступающие от вышестоящего пункта управления с интервалом 10 мин. Каждая задача управления характеризуется количеством объектов воздействия, по каждому из которых принято решение на осуществление воздействия, произведено распределение этих объектов между подчиненными элементами, сформирована команда на осуществление воздействия и доведена до подчиненных. Система позволяет создавать цепь процессов, соединенных между собой. Процессы в свою очередь задают последовательность операций, через которые проходят заявки.

Необходимо учесть, что единых подходов оценки эффективности [2, 3] нет – не только к обеспечению защиты информации, но и к построению самих систем и их компонентов. Поэтому необходимо разработать инструменты для определения подходов к построению систем защиты [5], так и для определения показателей ее эффективности.

При выборе показателя эффективности защиты информации нужно исходить из того, что эффективность управления защитой информации [4] оценивается с помощью показателя эффективности управления. Исходя из основного целевого назначения системы управления – своевременной выработки и реализации правильного управляющего воздействия на управляемый объект, показателем эффективности управления защитой информации Wэ целесообразно выбрать вероятность своевременного принятия и реализации правильного решения, обеспечивающего оптимальное использование возможностей подчиненных технических средств.

Трехуровневая модель обеспечивает полноту и логичность системы защиты информации в ГИС и  визуализирует качество функционирования системы во времени, что позволяет обеспечить эффективность процесса обеспечения управления безопасностью.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Селифанов В. В., Звягинцева П. А., Юракова Я. Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

2. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. – С. 109-113.

3. Селифанов В.В., Звягинцева П.А., Голдобина А.С., Исаева Ю.А. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты // Вестник СГУГиТ. – 2017. Т. 22, № 4. – С. 220–225.

4. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов,  Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015. – С. 208–213.

5. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. 2014. № 23. С. 188.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-25-29

# АНАЛИЗ РАЗВИТИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

***Оксана Владимировна Ермак***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (923)174-90-59, e-mail: oksana.ermak@inbox.ru

***Анна Владимировна Якунина***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)707-36-48, e-mail: aniyaaa99@mail.ru

***Карина Викторовна Яркова***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (961)219-75-46, e-mail: 61ka16@gmail.com

Процесс развития средств защиты информации можно разделить на три этапа: изобретение письменности, появление технических средств обработки информации и период массовой информатизации общества. Каждый этап характеризуется развитием носителей информации, в результате которого появляются новые угрозы утечки информации. В связи с этим возникает необходимость формирования требований к средствам защиты информации, информационных систем.

**Ключевые слова:**средство защиты информации, информация, требования, методы защиты информации, система, средство обработки информации, угроза утечки информации.

# ANALYSIS OF THE DEVELOPMENT OF MEANS OF INFORMATION PROTECTION

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

***Oksana V. Ermak***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (923)174-90-59, e-mail: oksana.ermak@inbox.ru

***Anna V. Yakunina***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (913)707-36-48, e-mail: aniyaaa99@mail.ru

***Karina V. Yarkova***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (961)219-75-46, e-mail: 61ka16@gmail.com

The process of the development of means of information protection can be divided into three stages: invention of writing, emergence of technical means of information processing and period of mass Informatization of society. Each stage is characterized by the development of information carriers, as a result of which there are new threats of information leakage. In this connection there is a necessity of formation of requirements to protection of information and information systems.

**Key words:** means of information protection, information, requirements, methods of information protection, system, means of information processing, threat of information leakage.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации [1], которое может обеспечивать защиту всех составных частей.

Процесс формирования методов и средств защиты информации можно поделить на три периода. Деление происходит на основе эволюции видов носителей информации.

С каждым годом финансовые потери, приносимые вирусными атаками на компьютерные сети становятся все больше. Наиболее известным примером является вирус «Iloveyou», так как данная «эпидемия» вывела из строя более 5 миллионов компьютеров и нанесла ущерб свыше 10 миллиардов долларов. Вирус распространялся через электронную почту пользователей MicrosoftOutlook и уничтожал или изменял некоторые файлы на зараженном компьютере. Кроме того, червь сразу же, в момент запуска, рассылал себя по всем адресам адресной книги пользователя [2].

Интересным фактом в сфере информационной безопасности является вывод о том, что утечка хотя бы 20 % информации, касающейся данных о коммерческой организации, в шестидесяти случаях из ста приводит к ее банкротству.

Гостехкомиссия России (сейчас Федеральная служба по техническому и экспортному контролю – ФСТЭК России) в период с 1992 по 1999 г. разработала пакет руководящих документов, посвященных вопросам защиты информации в автоматизированных системах. Также был разработан ГОСТ Р ИСО/МЭК 15408-2-2002, в котором описываются требования безопасности информационных технологий объекта оценки, излагаемых в профиле защиты или в задании по безопасности, на данный момент действует ГОСТ Р ИСО/МЭК 15408-2-2013 [3].

Для того, чтобы не происходила утечка данных, необходимо разрабатывать и своевременно обновлять требования к средствам защиты информации. Сейчас происходит постепенный переход к «требованиям нового поколения», которые пока представлены, следующим набором документов.

Приказ ФСТЭК России от 3 апреля 2018 г. №55. Положение о системе сертификации средств защиты информации [4], устанавливаливающее основные принципы, организационную структуру системы обязательной сертификации средств защиты информации, порядок проведения сертификации этих средств по требованиям безопасности информации, а также государственного контроля и надзора за сертификацией и сертифицированными средствами защиты информации.

Приказ ФСТЭК России от 15 марта 2012 г. №638. Требования к системам обнаружения вторжения [5]. Данные требования применяются к программным и программно-техническим средствам, которые используются для обеспечения защиты информации, составляющих сведения с ограниченным доступом.

Приказ ФСТЭК России от 1 августа 2012 г. №28. Требования к средствам антивирусной защиты [6]. Данные требования применяются к программным средствам, используемым в целях обеспечения защиты информации, которые содержат сведения ограниченного доступа.

Приказ ФСТЭК России от 1 января 2014 г. №119. Требования к средствам доверенной загрузки [7]. Данные требования к средствам доверенной загрузки применяются к программным и программно-техническим средствам, используемым для обеспечения защиты информации, которые содержат сведения ограниченного доступа и предотвращают несанкционированный доступ к программным и (или) техническим ресурсам.

Приказ ФСТЭК России от 1 декабря 2014 г. №87. Требования к средствам контроля съемных машинных носителей информации [8]. Данные требования применяются к программным и программно-техническим средствам, которые используются в целях обеспечения защиты информации, которые содержат информацию ограниченного доступа и предотвращают несанкционированный доступ к программным и (или) техническим ресурсам.

Приказ ФСТЭК России от 1 декабря 2016 г. №9. Требования к межсетевым экранам [9]. Данные требования применяются к программным и программно-техническим средствам, которые реализуют функции контроля и фильтрации и используются в целях обеспечения защиты информации, содержащей сведения ограниченного доступа.

Приказ ФСТЭК России от 1 июня 2017 г. №119. Требования безопасности информации к операционным системам [10]. Данные требования применяются к операционным системам, которые используются для обеспечения защиты информации, содержащей сведения ограниченного доступа при ее обработке в информационных системах.

Как видно, средствам обеспечения безопасного межсетевого взаимодействия, сейчас уделяется достаточно большое внимание. Эти средства должны учитывать все применяемые информационные технологии.

Вслед за бурным развитием информационных технологий появляются все новые и новые угрозы. Для того, чтобы им противостоять активно внедряются такие средства защиты как DLP и SIEM.

DLP-система (Data Loss Prevention) – это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети.

Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач:

— мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;

— контроль использования рабочего времени и рабочих ресурсов сотрудниками;

— выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность;

— контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.).

SIEM-системы появились в результате эволюции и слияния SEM и SIM.

SEM (Security Event Management) – система защиты, работающая в режиме реального времени. Она самопроизвольно отслеживает события в информационных потоках и собирает их.

SIM (Security Information Management) – система, отвечающая за анализ сведений на основе статистики и отклонений от установленных правил безопасности.

SIEM-решение позволяет обнаружить: внешние и внутренние атаки; отдельные заражения вирусами; попытки получить несанкционированный доступ к защищаемой информации; нарушения в работе информационных систем; слабые точки защиты; нарушения структуры средств защиты.

SIEM-система может: анализировать события и предупреждать при возникновении каких-либо отклонений; проверять на соответствие стандартам; создавать отчеты, в том числе настроенные пользователями; мониторить события от устройств или серверов и создавать соответствующие оповещения для заинтересованных лиц; избавлять от рисков при наличии сканера уязвимостей.

В то же время такие системы, как DLP и SIEM, не имеют четко установленных требований по информационной безопасности.

В связи с повлением новых тенденций в развитии информационных технологий становятся востребованными новые функции DLP-систем. Глобальное использование мобильных устройств при ведении бизнеса послужило причиной возникновения мобильного DLP. Создание корпоративных и публичных «облаков» потребовало защиты, в том числе и DLP-системами. Все это привело к появлению «облачных» сервисов инфоормационной безопасности.

Одной из компаний лидеров производителей DLP-систем из зарубежных компаний является Symantec Corp., на российском рынке популярны продукты отечественных разработчиков DLP-систем: Info Watch End Point Security, Sola rDozor.

На данном этапе многие крупные компании и государственные учреждения являются главными потребителями SIEM-систем. Так как они отвечают таким качествам, как: производительность, масштабируемость, отказоустойчивость также немаловажным фактором является соотношение «цена-качество». Государственные учреждения большое внимание уделяют на наличие сертификатов соответствия требованиям регуляторов.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р50922-2006 «Защита информации. Основные термины и определения» [Электронный документ] URL: http://www.altell.ru/legislation/standards/50922-2006.pdf.

2. Начало эпидемии ILOVEYOU [Электронный документ] URL: https://www.securitylab.ru/informer/240711.php.

3. ГОСТ Р ИСО/МЭК 15408-2-2013«Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий» [Электронный документ] URL: http://www.internet-law.ru/gosts/gost/6112/

4. Об утверждении Положения о системе сертификации средств защиты инфорации: приказ ФСТЭК России от 03.04.2018 №55 / [Электронный ресурс] / Режим доступа: www.consultant.ru

5. Об утверждении требований к системам обнаружения вторжений: информационное письмо ФСТЭК России от 01.03.2012 №240 / [Электронный ресурс] / Режим доступа: www.consultant.ru

6. Об утверждении требований к средствам антивирусной защиты: информационное сообщение ФСТЭК России от 30.07.2012 №240/24/3095 / [Электронный ресурс] / Режим доступа: www.consultant.ru

7. Об утверждении требований к средствам доверенной загрузки: информационное письмо ФСТЭК России от 06.02.2014 №240/24/405 / [Электронный ресурс] / Режим доступа: www.consultant.ru

8. Об утверждении требований к средствам контроля съемных машинных носителей информации: информационное сообщение ФСТЭК России от 24.12.2014 №240/24/4918 / [Электронный ресурс] / Режим доступа: www.consultant.ru

9. Об утверждении требований к межсетевым экранам: информационное сообщение ФСТЭК России от 28.04.2016 № 240/24/1986 / [Электронный ресурс] / Режим доступа: www.fstec.ru

10. Об утверждении требований безопасности информации к операционным системам: информационное сообщение ФСТЭК России от 18.10.2016 № 240/24/4893 / [Электронный ресурс] /Режим доступа: fstec.ru

УДК 004.415.535
DOI: 10.33764/2618-981X-2019-9-30-34

# ПРОВЕДЕНИЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

***Владимир Алексеевич Кривенцев***
Управление Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу, 630091, Россия, г. Новосибирск, Красный пр., 41, старший государственный инспектор, e-mail: kriventsev@list.ru

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

***Полина Александровна Звягинцева***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

Дается краткое описание состояния рынка отечественных операционных систем, которые могут проходить аттестацию в составе автоматизированной системы. Приводится описание того, что включают в себя аттестационные испытания объекта информатизации, программа аттестационных испытаний, методики аттестационных испытаний и протокол аттестационных испытаний.

**Ключевые слова:** аттестационные испытания, автоматизированная система.

# BENCHMARK TESTING OF A SECURE EXECUTION AUTOMATED SYSTEM

***Vladimir A. Kriventsev***
Department of the Federal Service for Technical and Export Control of the Siberian Federal District, 41, Krasny Prospect St., Novosibirsk, 630091, Russia, Senior State Inspector, e-mail: kriventsev@list.ru

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

***Polina A. Zviagintcheva***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

A brief description of the state of the market of domestic OS, which can be certified as part of the AU are given. In addition, the description of what includes certification tests of the object of Informatization, the program of certification tests, methods of certification tests and the Protocol of certification tests is made.

**Key words:** attestation tests, automated system.

На данный период времени в России осуществляется постепенный переход систем на продукцию отечественного производителя, в том числе в сфере информационной безопасности. Как правило, для таких систем характерно использование внутренних механизмов защиты и, соответственно, осуществляется переход на сертификацию ОС, как вида СЗИ [1].

В качестве объекта исследования берется система защиты автоматизированной системы, а как предмет исследования рассматривается система защиты автоматизированной системы от несанкционированного доступа.

В таком случае, единственным документом доступным для построения систем высокого уровня (средства защиты информации третьего класса и выше) является профиль защиты [2].

ИТ.САВЗ.Г2.ПЗ и ИТ.ОС.А2.ПЗ – документы, в которых изложены требования к безопасности конкретных средств и информационных систем.

ГОСТ РО 0043-003-2012 – «Аттестация объектов информатизации. Общие положения» [3].

ГОСТ РО 0043-004-2013 – «Аттестация объектов информатизации. Программа и методики аттестационных испытаний» [4].

Существующие средства защиты информации, а именно DallasLock, SecretNet, Страж и подобные им, сертифицированы и могут проходить в дальнейшем сертификацию по документу «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации», аттестационные испытания проводятся по документу «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации». Данные документы между собой коррелируются [5, 6].

Для прохождения аттестации средства защиты информации должны быть сертифицированы. Таким образом, получается, что средства защиты информации имеют сертификацию по классу защищенности, а не по классу защиты, как это требуют приказы ФСТЭК. В соответствии с этим существуют только профили защиты, которые удовлетворяют данным требованиям.

Одна из проблем заключается в том, что необходимо подобрать такую операционную систему, которая удовлетворяла бы всем требованиям, выдвигаемым к системам такого класса [7].

В ходе исследования данной темы был произведен сравнительный анализ операционных систем российской разработки, а именно:

- «Astra Linux Special Edition»;
- РОСА DX «КОБАЛЬТ» 1.0;
- МСВСфера 6.3 АРМ;
- «Циркон 36К»;
- Альт Линукс СПТ 6.0.

Стоит отметить, что все представленные операционные системы способны осуществлять управление доступом к различным изделиям, входящим в состав современных автоматизированных систем.

Сравнительный анализотечественных операционных систем приведен в таблице.

| | AstraLinux Special Edition | РОСА DX «КОБАЛЬТ» 1.0 | МСВ Сфера 6.3 АРМ | Циркон 36К | Альт Линукс СПТ 6.0 |
|---|---|---|---|---|---|
| Ядро ОС | Linux 4.2.0 | Linux 3.0.69 | CentOS 6.7 | CentOS GNU/Linux 6.5 | Linux 2.6.32 |
| Базовый дистрибутив | Debian | Mandriva Linux (Red Hat Linux) | Red Hat Linux | Red Hat Enterprise Linux | Red Hat Linux |
| РД СВТ | 2 класс тип А | 5 класс | - | 5 класс | 4 класс |
| РД НДВ | 2 уровень | 4 уровень | 4 уровень | 4 уровень | 3 уровень |
| РД АС | 1Б | 1Г | 1Г | 1Г | 1В |

«AstraLinux SpecialEdition» сертифицирована в системах сертификации средств защиты информации Минобороны, ФСТЭК и ФСБ России, а также включена в единый реестр российских программ Минкомсвязи России.

В настоящее время при аттестации автоматизированной системы [3] на соответствие требованиям по безопасности информации, функции, которые реализует операционная система, как средство защиты от несанкционированного доступа, должны соответствовать требованиям класса защищенности 1Б [6].

Аттестационные испытания объекта информатизации включают:

а) анализ

- структуры объекта информатизации;
- комплекса технических средств;
- программного обеспечения;
- системы защиты информации.

б) проверку наличия сертификатов соответствия на продукцию, используемую в целях защиты информации;

в) аттестационные испытания системы защиты информации объекта информатизации в реальных условиях эксплуатации;

г) оформление протоколов аттестационных испытаний. Протоколы подписывают специалисты, проводившие испытания, и утверждает орган по аттестации. Протоколы должны содержать описание проведенных измерений, испытаний, расчетов, а также их результаты и выводы о соответствии этих результатов требованиям безопасности информации;

д) оформление заключения по результатам аттестационных испытаний. Заключение подписывается членами аттестационной комиссии, утверждается органом по аттестации и доводится до заявителя.

Программа аттестационных испытаний АС содержит перечень конкретных работ, которые требуется провести для оценки и подтверждения выполнения предъявляемых требований безопасности информации.

Программа аттестационных испытаний АС включает:

- проверку структуры, состава и условий эксплуатации АС;
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям;
- аттестационные испытания системы защиты информации объекта информатизации в реальных условиях эксплуатации;

− проведение испытаний АС на соответствие требованиям по защите информации от несанкционированного доступа;

− подготовку отчетной документации и оценку результатов испытаний аттестуемой АС;

− оформление материалов аттестационных испытаний.

Методики аттестационных испытаний должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке системы защиты информации, перечень требований, подлежащих проверке и условий, в которых проводится проверка.

Методики аттестационных испытаний АС должны включать:

− описание и порядок выполнения практических действий;

− перечень требований, подлежащих проверке и условий, в которых проводится проверка;

− критерии, по которым делаются выводы о соответствии аттестуемого объекта информатизации требованиям безопасности информации на каждом этапе проводимых работ.

Протокол аттестационных испытаний должен включать:

− вид испытаний;

− объект испытаний;

− дату и время проведения испытаний;

− место проведения испытаний;

− перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);

− перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

− результаты измерений.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов [9].

Таким образом можно сказать, что выбор операционных систем для аттестации АС по требованиям класса 1Б очень мал и на данный момент среди операционных систем отечественной разработки существует лишь одна, которая удовлетворяет этому требованию, а именно AstraLinux Special Edition 1.5. Помимо этого, у данной системы есть ряд преимуществ, а именно она сертифицирована в системах сертификации средств защиты информации Минобороны, ФСТЭК и ФСБ России и включена в единый реестр российских программ Минкомсвязи России. Система уже введена в действие и на ней построена информационная система Национального центра управления обороной РФ [10,11].

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения» от 1 апреля 2015 № 96.

2. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

3. ГОСТ РО 0043-003-2012. Аттестация объектов информатизации. Общие положения.

4. ГОСТ РО 0043-004-2013. Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

5. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» утвержденный решением председателя Гостехкомиссии России от 1992 г.

6. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденный решением председателя Гостехкомиссии России от 30.05.1992 г.

7. Приказ ФСТЭК России № 55 от 3 апреля 2018 г. «Положение о системе сертификации средств защиты информации».

8. Информационное Сообщение ФСТЭК России об утверждении Требований безопасности информации к операционным системам от 18 октября 2016 г. № 240/24/4893.

9. Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено председателем Гостехкомиссии России 25.11.1994 – М.: Гостехкомиссия РФ, 1994.

10. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности сборник статей Международной научно-практической конференции. 2016. – С. 109-113.

11. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 220–225.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-35-38

# ОСОБЕННОСТИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

***Софья Васильевна Степанова***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (913)459-34-90, e-mail: stepanova.sofya@mail.ru

***Никита Алексеевич Стрихарь***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (996)387-72-77, e-mail:strihar.nikita@mail.ru

В статье рассматриваются особенности выбора средств защиты информации я государственных информационных систем. Рассмотрены основные виды СЗИ, которые использовались на территории России раньше, а также средства, используемые сейчас. Приведены результаты работ, проведенных ФСТЭК и ФСБ России, относительно введения классификации СЗИ и мер, которые предпринимаются оператором ГИС. Определены тенденции развития и создания новых средств защиты информации.

**Ключевые слова:** информационная безопасность, средства защиты информации, государственные информационные системы.

# CHOICE OF MEANS OF PROTECTION OF INFORMATION IN STATE INFORMATION SYSTEMS

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, Russia, 630108, Associate Professor, Department Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

***SofyaV. Stepanova***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, Russia, 630099, Bachelor of Information Security, phone: (913)459-34-90, e-mail: stepanova.sofya@mail.ru

***Nikita A. Strigari***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, Russia, 630099, Bachelor of Information Security, phone: (996)387-72-77, e-mail: strihar.nikita@mail.ru

The article discusses the features of the choice of information security tools for state information systems. The main types of SPI, which were used on the territory of Russia before, as well

as the means used now, are considered. The results of work, carried out by the FSTEC and FSB of Russia, on the introduction of the classification of SPI and measures taken by the GIS operator are presented. Tendencies of development and creation of new means of information protection are defined.

**Key words:** information security, means of information protection, state information systems.

Развитие науки и техники не останавливается. Это обусловлено тем, что люди стараются найти более продуманные, современные и выгодные решения. Данная тенденция распространяется и на сферу обеспечения защиты информации. Ежедневно появляются новые вирусы, совершаются различного рода хакерские атаки и взломы. Чтобы обезопасить систему, специалист по информационной безопасности обязан разбираться в тенденциях и новинках в своей сфере деятельности. Также, он должен грамотно подходить к выбору средств защиты информации, учитывая цели, особенности и возможности организации. Это касается и особенностей выбора средств защиты информации в государственных информационных системах.

Применение средств защиты информации существенно повышает уровень защиты от несанкционированного доступа. Однако, реализовать необходимый уровень защищенности возможно только при использовании сертифицированных средств защиты информации. В данной работе, разобраны проблемы выбора средств защиты информации, на основе существующих требований ФСТЭК России.

Раньше существовал ограниченный набор средств защиты информации (СЗИ). Туда входили средства вычислительной техники (СВТ) – программные и технические элементы систем обработки данных, способные функционировать самостоятельно или в составе других автоматизированных систем (АС) [5]. Существуют следующие виды средств защиты информации: технические средства и системы в защищенном исполнении, технические средства защиты информации от несанкционированного доступа (НСД) (замки, пломбы), программные средства защиты информации от НСД (антивирусные программы), защищенные программные средства обработки информации (программные средства автоматизированных систем управления), программно-технические средства защиты информации, специальные средства защиты от идентификации личности (средства защиты от дактилоскопической экспертизы) [1].

Существует семь классов защищенности СВТ от несанкционированного доступа к информации, для государственных информационных систем подходит пятый класс. Он отличается наличием дискреционного управления доступом: возможностью устанавливать права доступа пользователей к различным ресурсам. Следующим пунктом в процессе обеспечения защищенности информации является установка межсетевых экранов – средств, реализующих контроль за информацией, поступающей и выходящей из АС. Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты. В отношении государственных информационных систем (ГИС) рассматриваются 4 и 5 классы защищенности [3].Также для каждой

ГИС разрабатываются и утверждаются технические условия, которые могут включать в себя: требования к составу технических средств и операционной системе, наличие модуля доверенной загрузки, антивирусного решения и так далее.

Данные требования к средствам защиты информации, разработанные в начале 90-х годов, уже устарели, так как на тот момент не существовало документов, регулирующих выполнение тех требований. Начиная с 2011 года ФСТЭК России начал реализацию деятельности, направленной на изменение подходов к защите информации. Так, например, для государственных информационных систем были установлены три класса защищенности, а также требования к каждому из них. Класс защищенности определяется в зависимости от уровня значимости информации, обрабатываемой в ИС и ее масштаба. В приказе ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 15 февраля 2017 г. № 27) приведен состав мер по защите информации для каждого класса защищенности информационных систем [2].

Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия: формируются требования к защите информации, разрабатывается и внедряется система защиты информации для ИС, проводится аттестация ИС. ФСТЭК выпустил ряд документов, систематизирующих классификацию СЗИ, а также описывающих тот или иной класс. Приказами ФСТЭК России были утверждены требования к системам обнаружения вторжений, межсетевым экранам, средствам антивирусной защиты, средствам контроля съемных машинных носителей, введена классификация операционных систем для обеспечения защиты информации. ФСБ России, определила классы криптографических СЗИ и средств защиты электронной подписи [4]. На данный момент существует государственный реестр сертифицированных СЗИ, поддерживаемый ФСТЭК России. Аналогичный перечень сертифицированных СЗИ имеет и ФСБ России в рамках своей компетенции.

Здесь необходимо помнить, что надежную защиту информации, обеспечит комплексное решение, включающие соответствующие средства защиты.

Так как веб-сервисы и их структура постоянно развиваются, на этой почве возникла потребность в создании новых решений по защите информации. Одним из таких решений стал WebApplicationFirewall (WAF) – экран для защиты веб-приложений.

Продвинутые модели WAF могут анализировать XML, JSON и другие протоколы современных порталов и мобильных приложений. Это позволяет противодействовать обходу межсетевого экрана, что является важным, так как большое количество людей имеет доступ к ГИС. В качестве примера можно привести портал «Госуслуги», для регистрации на котором гражданину необходимо вводить личные данные. В этом случае использование WAF в роли СЗИ поможет предотвратить большое количество проблем. В качестве другого примера можно привести использование личного кабинета на сайте банка. Пользователь заходит на сайт, проходит там аутентификацию, а в другой вкладке открывает ресурс, который оказывается зараженным. JavaScript, загрузившийся в другом

окне, может запросить информацию о переводе денежных средств и браузер предоставит все необходимые параметры для осуществления финансовой транзакции, так как сеанс связи пользователя с банком еще не окончится. Таким образом можно выявить слабые стороны в алгоритме аутентификации. Проблему можно избежать, если для каждой формы, содержащейся на странице сайта, будет генерироваться уникальный токен. Некоторые WAF могут самостоятельно внедрять подобную защиту в веб-формы и защищать, таким образом, клиента – а вернее, его запросы, данные, URL и cookie-файлы. В ходе работы WAF запускается основной компонент защиты – машинное обучение, которое характеризуется способностью понимать группы протоколов и зависимостей, свойственных для веб-приложений, которые строятся над прикладными протоколами http/https. Таким образом формируется список допустимых идентификаторов доступа [6].

Межсетевой экран Positive Technologies Application Firewall, предназначенный для защиты от кибератак, успешно прошел сертификационные испытания ФСТЭК России. Данный межсетевой экран стал первым решением в классеWAF, подтвердившим соответствие требованиям технических условий и руководящих документов по четвертому уровню контроля отсутствия недекларированных возможностей. Наличие сертификата означает, что данный межсетевой экран может применяться в государственных информационных системах до первого класса защищенности включительно (в соответствии с приказом ФСТЭК России от 11.02.2013 № 17) и ИСПДн до первого уровня защищенности включительно (согласно приказу ФСТЭК России от 18.02.2013 № 21) [7].

В настоящее время идет большая работа по изменению требований к средствам защиты информации. Каждый год документально оформляются новые виды средств защиты, с целью обеспечить безопасность всех применяемых информационных технологий.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ ФСБ РФ от 13.11.1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

2. Приказ ФСТЭК РФ от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»(ред. от 15.02.2017 г. № 27).

3. Приказ ФСТЭК РФ от 9.02.2016 г. № 9 «Требования к межсетевым экранам».

4. Приказ ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

5. ФСТЭК РФ. «Руководящий документ. Решение председателя Гостехкомиссии России от 30.03.1992 г.».

6. Чем защищают сайты, или зачем нужен WAF? [Электронный ресурс] – Режим доступа: https://habr.com/company/pt/blog/269165/.

7. PT ApplicationFirewall сертифицирован ФСТЭК России [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/43455/.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-39-41

# ПРОБЛЕМА ОПРЕДЕЛЕНИЯ ПЕРЕЧНЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

***Владислав Сергеевич Сысалов***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (913)459-42-11, e-mail: 79134594211@yandex.ru

***Денис Константинович Кричевский***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (963)947-39-13, e-mail: Kinstk9@gmail.com

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

В статье поднимается проблема разработки перечня объектов критической информационной инфраструктуры и их категорирования в научной деятельности высших учебных заведений.

**Ключевые слова:** критическая информационная инфраструктура, высшее учебное заведение, категорирование.

# PROBLEM OF DETERMINING THE LIST OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

***Vladislav S. Sysalov***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, BSc of Information Security, phone: (913)459-42-11, e-mail: 79134594211@yandex.ru

***Denis K. Krichevsky***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, BSc of Information Security, phone: (963)947-39-13, e-mail: Kinstk9@gmail.com

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo, St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

The article raises the problem of formation of a list of objects of critical information infrastructure and their categorization in the scientific activity of higher educational institutions.

**Key words:** critical information infrastructure, higher education institution, categorization.

В соответствии со 2-ой статьей Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», под объектом критических информационных инфраструктур (КИИ) понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

В той же статье приводится определение субъекта критической информационной инфраструктуры – это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [1].

Основными органами, осуществляющими функции регулирования и надзора за исполнением данного федерального закона, являются ФСТЭК России и ФСБ России.

ФСТЭК России: ведет реестр значимых объектов КИИ; устанавливает требования по обеспечению безопасности значимых объектов КИИ; контролирует выполнение требований по категорированию объектов КИИ и обеспечению безопасности значимых объектов.

ФСБ России: устанавливает порядок информирования об объектах КИИ и инцидентах, определяет состав предоставляемой информации; обеспечивает установку на объектах КИИ технических средств ГосСОПКА и устанавливает требования к ним; проводит оценку безопасности объектов КИИ.

На данном этапе основная задача субъектов КИИ – определение перечня объектов и их категорирование. Как показывает практика многие субъекты с этим не справляются.

Рассмотрим сферу науки, а именно высшие учебные заведения (вуз). В настоящее время, подавляющее их большинство помимо образовательных функций ведет и научную деятельность, и, следовательно, относится к субъектам КИИ.

При этом в указанных учебных заведениях есть подразделения, на которые возложены, в том числе, и научные функции. Это могут быть научно-исследовательские институты, научно-исследовательские лаборатории и кафедры. В их деятельности используются информационные системы, например, реализующие моделирование тех или иных процессов, такие как «Mathcad» и «AnyLogic».

Можно сделать вывод, что подавляющее большинство вузов является субъектами КИИ, и попадает под требования законодательства Российской Федерации о безопасности КИИ.

При этом, несмотря на то, что требования Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» вступили в силу более года назад, подавляющее большинство высших учебных заведений работу по разработке перечней объектов КИИ еще не начинало.

Здесь стоит отметить, что разработка перечня объектов КИИ, сама по себе не несет дополнительных расходов, проводится собственными силами и автоматически не означает, что организациям придется нести какие-либо финансовые траты.

Проведенная работа в ряде Новосибирских вузов, а именно в Сибирском государственном университете геосистем и технологий и Новосибирском государственном университете экономики и управления «НИНХ», показала, что в них отсутствуют объекты КИИ, которые требуют присвоение категории значимости.

Стоит отметить, что разработка перечня объектов КИИ является не только выполнением требований законодательства Российской Федерации, но и своеобразным свидетельством, о том, что вуз официально имеет информационные системы для работы в научной сфере. А, следовательно, возможность участия вуза, который не имеет информационных систем, с помощью которых он может проводить научные исследования, во внешнем гранте, выглядит сомнительно.

Таким образом, реализация требований в области безопасности КИИ для вузов является жизненной необходимостью.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

2. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3. Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

УДК 004.9, 003.26, 004.056, 34.096
DOI: 10.33764/2618-981X-2019-9-42-46

# ПОСТРОЕНИЕ ЮРИДИЧЕСКИ ЗНАЧИМОГО ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ БЛОКЧЕЙН В ИНФОРМАЦИОННЫХ СИСТЕМАХ

***Любовь Денисовна Заворина***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)746-00-96, e-mail: ljubasik-1234@mail.ru

***Анастасия Алексеевна Ерохина***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)488-50-46, e-mail: eroxina1997@bk.ru

***Диана Георгиевна Макарова***
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: kaf.ib@ssga.ru

В статье рассматривается проблема системы электронного документооборота с использованием технологии «Блокчейн» для государственных органов, а именно, для критической информационной инфраструктуры. Данная проблема является актуальной, поскольку развитие цифровой экономики в России уже достигло уровня правительства.

**Ключевые слова:** критическая информационная инфраструктура, блокчейн, цифровая экономика, информационная система.

# BUILDING OF A LEGALLY SIGNIFICANT PROTECTED DOCUMENT MANAGEMENT BASED ON BLOCKCHAIN IN INFORMATION SYSTEMS

***Lyubov D. Zavorina***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (913)746-00-96, e-mail: ljubasik-1234@mail.ru

***Anastasia A. Erokhina***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Student, phone: (913)488-50-46, e-mail: eroxina1997@bk.ru

***Diana G. Makarova***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: kaf.ib@ssga.ru

The article deals with the problem of electronic document management system using "Blockchain" technology for public authorities, namely for critical information infrastructure. The problem is relevant since the development of the digital economy in Russia has already reached the governmental level.

**Key words:** critical information infrastructure, blockchain, digital economy, information system.

Совсем скоро нас ждет эра цифровой экономики – системы экономических, социальных и культурных отношений, которая основана на инженерии компьютерных систем, математике и криптографии. Основной задачей цифровой экономики является улучшение качества жизни граждан.

Главное преимущество нововведения – математический алгоритм блокчейн, который позволяет вести надежный учет финансов, денежных расчетов, и даже операций с материальными и нематериальными активами. Эта уникальная технология делает возможным записать в цифру все то, что так важно человеку, безопасно хранить и передавать друг другу, минуя посредников. Благодаря глобальной бухгалтерской книге, которая позволяет фиксировать историю транзакций, стало невозможным подделать состояние счетов. Таким образом, в мире блокчейн доверие возникнет из сети.

Первоначальное появление технологии блокчейн в качестве инструмента для проведения транзакций с электронной валютой «биткоин» получило развитие как обособленная технология, которая может использоваться за рамками криптовалют. В России (далее – РФ) она получила название технологии распределенного реестра (англ.: Distributed ledger technology – DLT).

Блокчейн обладает преимущественными функциями безопасности, а именно:

– защищенность (данные шифруются для подтверждения транзакций);

– неизменность (от предшествующих транзакций зависит текущее состояние блокчейн);

– прозрачность (обеспечивается публичным и распределенным хранением) [1].

Таким образом, технология блокчейн может способствовать защите государственных интересов.

В начале 2016 г. в Великобритании был опубликован отчет «Технология распределенных реестров: за рамками блокчейн», представляющий исследование, проведенное Государственным управлением науки под руководством главного научного советника Правительства Великобритании Ричарда Кастеляйна (Richard Kastelein). В отчете отмечается, что главная задача государства заключается в разработке четкой концепции того, как технология распределенных реестров может улучшить деловые процессы государственных органов, и каким образом она может быть использована для оказания услуг гражданам. Государство должно выступить в роли продвинутого заказчика, внедряющего эту технологию. Поступая таким образом, государство может поддерживать и влиять на развитие экономической активности в этом секторе.

По мнению специалистов, занимающихся анализом технических решений в области блокчейн-технологий, на данный момент существуют следующие возможные проблемы:

– обеспечение требуемой пропускной способности сети для нормальной работы блокчейна;

– предоставление узлу необходимого дискового пространства из-за непрерывной генерации блоков.

Для использования технологии блокчейн в государственной сфере должны быть внесены изменения в нормативно-правовые акты РФ в сфере информационных технологий. Для определения таких изменений, Минэкономразвития России 17 октября 2017 г. подготовило Проект Постановления Правительства РФ «О проведении на территории г. Москвы эксперимента по использованию технологии «Блокчейн» в целях мониторинга достоверности сведений Единого государственного реестра недвижимости». Целями эксперимента являются определение эффективности и результативности использования технологии блокчейн, определение изменений, которые необходимо внести в нормативно-правовые акты РФ в сфере информационных технологий, определение технических возможностей информационной системы по использованию технологии блокчейн.

Изменения могут коснуться Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», регулирующего отношения в области обеспечения безопасности критической информационной инфраструктуры РФ (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

Объектами КИИ, согласно вышеупомянутому закону, являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. На данный момент идет определение точного перечня объектов КИИ. Одним из субъектов КИИ стали государственные органы, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (например, Минздрав НСО) [2].

Если блокчейн включить в список объектов КИИ, то его безопасность будет регулироваться данным законом.

Так как, в блокчейн все операции совершаются над цифровыми объектами, то необходимы изменения в законодательстве о регулировании оборота цифровых прав и цифровых денег, для совершения и исполнения сделок в так называемой цифровой среде. 26 марта 2018 г. в Государственную Думу был внесен законопроект №424632-7 о внесении изменений в части первую, вторую и четвертую Гражданского Кодекса РФ (о цифровых правах). В соответствии с проектом закона под «цифровым правом» понимается совокупность электронных данных (цифровой код), которая удостоверяет права на объекты гражданских прав. Принятие законопроекта позволит не только закрепить отправные гражданско-правовые нормы для регулирования оборота цифровых прав и цифровых денег, совершения и исполнения сделок в так называемой цифровой среде, но и позволит решить целый ряд других задач. В частности, будет обеспечена судебная защита прав, возникающих в отношениях по поводу таких объектов.

Технологию блокчейн можно внедрить в работу государственных органов, таким образом, она (технология) заменит работу информационной системы.

Чтобы сделать работу блокчейн более эффективной и удобной, необходимо понять, как используется информационная система.

Важнейшее место в работе государственных органов занимает электронный документооборот, построенный с использованием цифровой подписи. Фактически, электронный документооборот – это обмен документами в электронном виде. Информация, которая циркулирует в государственных органах, может носить конфиденциальный характер, следовательно, попадая в общедоступную сеть, она нуждается в защите. Электронная подпись решает следующие задачи:

– защита документов от модификации и подделки;

– определение автора документа, а также подлинности документа;

– обеспечение юридической силы документов;

– защита документов от несанкционированного просмотра.

Система электронного документооборота может строиться с использованием технологии блокчейн. Для этого необходимо разработать распределенное приложение для государственных органов на блокчейн-платформе Ethereum. Ethereum – конструктор для создания решений на блокчейн [3].

Для того, чтобы внедрить распределенное приложение в информационные системы государственных органов, оно должно соответствовать требованиям ФСБ России и ФСТЭК России.

Для начала опишем требования к информационной технологии Электронная подпись (ЭП):

– показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

– создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

– показывать информацию о внесении изменений в подписанный ЭП электронный документ;

– указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Теперь сформулируем требования к блокчейн по информационной безопасности для возможности применения в государственных органах [5–9]:

– сопоставление пользователя с устройством. Идентифицированная система (приложение) должна включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется с выделенным устройством [2];

– аутентификация и идентификация. Система должна требовать от пользователей идентифицировать себя при запросах на доступ и подвергать проверке подлинность идентификации – осуществлять аутентификацию;

– использование ассиметричного механизма электронной подписи для работы в приложениях на основе блокчейн. Данное требование устранит возможность использования пользователями сотен открытых ключей;

– документ, заверенный электронной подписью, должен читаться только при использовании ключа;

– открытый ключ (электронная подпись) должен передаваться вместе с документом.

## БИБЛИОГРАФИЧЕСКИЙСПИСОК

1. МеланиСвон (MelanieSwan). Блокчейн. Схема новой экономики (Blockchain: Blueprintfora New Economy). – М: Олимп-Бизнес, 2016. – 240 с.

2. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа кинформации», утвержденный решением председателя Государственной техническойкомиссии при Президенте Российской Федерации от 30 марта 1992 г.

3. Тапскотт Дон, Тапскотт Алекс. Революция блокчейн. Как технология, стоящая за биткоин, меняет деньги, бизнес и мир. – М: SmartReading, б.г. – 20 с.

4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

5. Селифанов В. В., Звягинцева П. А., Юракова Я. Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

6. Селифанов В.В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа [Текст] // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. – С. 109–113.

7. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГИТ. – 2017. – Т. 22, № 4. – С. 220–225.

8. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов, Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015. – С. 208–213.

9. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. – 2014. – № 23.– С. 188.

УДК 004.056.5
DOI: 10.33764/2618-981X-2019-9-47-53

# РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ МОБИЛЬНЫХ И ВЕБ-ПРИЛОЖЕНИЙ

***Анастасия Евгеньевна Мельникова***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (999)463-88-33, e-mail: knock1e@yandex.ru

***Игорь Николаевич Карманов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Актуальность темы работы обусловлена тем, что тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является популярной во всем мире услугой в области информационной безопасности (ИБ). Суть таких работ заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор выполняет роль злоумышленника, мотивированного на нарушение ИБ сети заказчика. В работе подробно изучены особенности проведения тестирования на проникновение, выполнен детальный анализ существующих зарубежных решений в области тестирования на проникновение, разработана собственная методика и предложены рекомендации по улучшению имеющихся методик.

**Ключевые слова:** тестирование на проникновение, разработка методики, информационная безопасность, мобильные приложения, веб-приложения, уязвимость, аудит.

# DEVELOPMENT OF THE METHODOLOGY FOR PENETRATION TESTING OF MOBILE AND WEB APPLICATIONS

***Anastasia E. Melnikova***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (999)463-88-33, e-mail: knock1e@yandex.ru

***Igor N. Karmanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Phisics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

The relevance of the topic is due to the fact that penetration testing (tests to overcome protection, penetration testing, pentest) is a worldwide popular service in the field of information security. The essence of such work is an authorized attempt to circumvent the existing set of protection means of information system. During testing, the auditor performs the role of an attacker motivated to violate the information security of customer's network. In article, features of penetration testing are thoroughly studied, a detail analysis of existing foreign solutions in the field of penetration testing is performed, a proprietary technique is developed and recommendations for improving the existing techniques are proposed.

**Key words:** penetration testing, methodology development, information security, mobile applications, web applications, vulnerability, audit.

## *Введение*

Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является чрезвычайно популярной во всем мире услугой в области ИБ. Суть таких работ заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор выполняет роль злоумышленника, мотивированного на нарушение ИБ сети заказчика.

Целью работы является разработка, апробация и выработка рекомендаций по совершенствованию методики тестирования на проникновение мобильных и веб-приложений.

## *Методы и методики*

Тестирование на проникновение не ограничивается простым обнаружением способов, которыми преступник может получить несанкционированный доступ к конфиденциальным данным или захватить системы в злонамеренных целях. Тестирование также имитирует атаку в реальных условиях, чтобы определить возможную величину ущерба и необходимые средства обеспечения защиты информации [1].

Комплексное тестирование на проникновение включает несколько областей:

– тестирование на проникновение в приложения – выявляет недостатки прикладного уровня (подделка межсайтовых запросов, межсайтовое выполнение сценариев, дефекты внедрения уязвимого программного кода, управление слабыми сеансами, небезопасные прямые ссылки на объекты и т.д.) [2];

– тестирование на проникновение в сеть – выявление уязвимостей на уровне сети и системы (неверные конфигурации, уязвимости для конкретного продукта, уязвимости беспроводной сети, мошеннические службы, слабые пароли и протоколы);

– тестирование на физическое проникновение (вторжение) – взлом физических барьеров (замки, датчики, камеры и т.д.);

– IoT (тестирование проникновения в устройства Интернета вещей) – выявление аппаратных и программных недостатков (слабые пароли, небезопасные протоколы, программный интерфейс приложения (API) или каналы связи, неверные конфигурации и т.д.) [3].

Рассмотрим несколько популярных методологий для проведения тестирования на проникновение (табл. 1).

Первая методология, «Technical Guide to Information Security Testingand Assessment», создана и поддерживается подразделением NIST(National Institute of Standards and Technology) – Computer Security Resource Center, центром по компьютерной безопасности, объединяющим специалистов федеральных служб, университетов, крупнейших ИТ-компаний США [4–5]. Последняя вер-

сия данной методологии выпущена в 2008 году и используется до сих пор, несмотря на то, что данные в ней устарели и нуждаются в детальной доработке [6].

*Таблица 1*

Сравнительная таблица актуальности методологий

| Разработчик | Наименование | Год выпуска |
|---|---|---|
| National Institute of Standards and Technology | Technical Guide to Information Security Testing and Assessment | 2008 |
| Institute for Security and Open Methodologies | Open Source Security Testing Methodology Manual 3 | 2010 |
| Open Web Application Security Project | Testing Guide | 2014 |

Ассоциация ISECOM (Institute for Security and Open Methodologies) опубликовала методологию «Open Source Security Testing Methodology Manual» (OSSTMM) – «Руководство по методологии тестирования безопасности с открытым исходным кодом» версии №3 в 2010 году. Это достаточно формализованный и хорошо структурированный документ, по настоящее время используемый в некоторых компаниях, предоставляющих услуги по ИБ [7–10]. С версии 3 OSSTMM охватывает тесты по всем каналам утечки информации – человеческий, физический, беспроводной, телекоммуникационный и сети передачи данных. Разработка OSSTMMv4 ведется в данный момент, но пока точных сроков публикации не назначено.

Open Web Application Security Project (OWASP) – открытый проект обеспечения безопасности веб-приложений. Последняя версия «TestingGuide» датируется 2014 годом, что также является совершенно недопустимым в современных реалиях [11–12]. Разработка новой версии активно ведется на сервисе хранения исходного кода Github, но даже примерные даты релиза отсутствуют [13–14].

Таким образом, как бы ни были хороши существующие решения, с их актуальностью имеются большие проблемы. Все рассмотренные методологии тестирования на проникновения очень сильно устарели. Следовательно, предприятию, которое оказывает услуги тестирования на проникновение, необходимо разработать собственную методику, используя в качестве базы существующие наработки.

## *Результаты*

При внешней и внутренней проверке безопасности исполнитель изучает возможные пути доступа в систему. Исполнитель будет использовать интерактивные методы тестирования [15].

Исполнитель проверяет согласованные с заказчиком IP-адреса и, в частности, предлагаемые на них сервисы в шесть этапов. Порядок проведения проверки показан на рисунке. Исполнитель проводит тестирование в информационной среде заказчика [16].


Этапы анализа защищенности

В итоге, предлагаемая методика включает следующие этапы:

- сбор информации – на первом этапе проводится сбор максимального количества информации из общедоступных баз данных (DNS, Whois, и т.д.), а также других источников (веб-сайт Заказчика, поисковые системы и т.д.), чтобы узнать о том, как можно эффективно атаковать конкретную организацию;
- сканирование портов – подлежащая проверке система подвергается процессу автоматического сканирования портов;
- анализ сервисов – сервисы, выявленные в ходе предыдущего этапа, подлежат изучению Исполнителем на предмет наличия уязвимостей в системе обеспечения безопасности заказчика. Тестирование охватывает как стандартные продукты (Microsoft IIS, ApacheWebserver, и т.д.), так и программное обеспечение, разработанное самим заказчиком или третьими лицами;
- уязвимости протокола канального уровня – проблемы безопасности в пределах второго уровня OSI-модели [17–18];
- уязвимости протоколов сетевого и транспортного уровней – проблемы безопасности в пределах третьего, четвертого и пятого уровней OSI-модели;
- проблемы межсетевого экрана (firewall) – проблемы безопасности, связанные с конфигурацией сетевого устройства защиты;
- конфигурация сервера – эта категория охватывает ошибки конфигурации для всех видов серверного программного обеспечения. Возможно использование известных уязвимостей, даже при наличии доступных обновлений;
- проблемы аутентификации и авторизации – приложение не обеспечивает достаточные средства аутентификации и/или авторизации для защиты своих ресурсов. Неавторизованный или не имеющий привилегий пользователь может получить доступ к ресурсам, которые защищены или должны быть защищены;
- проблемы бизнес-логики – злоумышленник может нарушить бизнес-логику приложения. Конкретные схемы попыток нарушения защиты зависят от конкретного приложения [19];
- раскрытие информации – злоумышленник может собирать информацию о внутреннем содержании приложения или конфигурации серверов;
- организация атак со стороны клиента (веб-браузер) – эта категория уязвимостей связана с сетью Интернет. Она охватывает атаки, нацеленные на веб-браузер;
- проблемы внедрения интерпретаторов/проверки вводимых значений – Приложение пропускает непроверенные параметры входящего потока в базу данных, ИПП операционной системы или другие интерпретаторы [20];

- проблемы управления соединением и небезопасное управление доверительными данными – переменные, участвующие в формировании соединения, могут быть использованы нецелевым образом. Злоумышленник может манипулировать доверительными данными или внутренними данными приложения;
- использование недокументированного или небезопасного функционала приложений, небезопасные алгоритмы – использование данных приложений изначально являются небезопасным. Использование небезопасных алгоритмов подвергает риску конфиденциальные данные;
- уязвимость к атакам на отказ в обслуживании – в результате атаки сервис может стать временно недоступным для использования;
- вторжение в сервисы из сети Интернет – выявленные уязвимости используются с целью получения доступа к системе. Анализ найденных уязвимостей позволяет исключить ложные опасности/аспекты, не представляющие реальной проблемы;
- оценка рисков – на основании результатов предыдущего этапа, сначала с использованием шкалы оценки риска определяется уровень риска каждой отдельной уязвимости и далее – общий риск, которому подвергается система.

По окончании оказания услуг заказчику в бумажном виде предоставляются консультационные и рекомендационные материалы по оптимизации настройки программных и аппаратных комплексов с целью устранения выявленных уязвимостей и общего повышения уровня безопасности информационных систем клиентов. Для каждого класса исследуемых уязвимостей необходимо составить таблицу, в которой будут отражены все виды уязвимостей. Обязательно требуется указать те уязвимости, на которые эксперт по ИБ проводил тестирование и те, которые в конечном итоге получилось успешно проэксплуатировать. Пример оформления приведен в табл. 2.

*Таблица 2*

Демонстрация исследованных и проэксплуатированных уязвимостей

| | Проблемы с интерпретатором / проверкой ввода | |
|---|---|---|
| | Приложение передает входные параметры в базу данных, API операционной системы или другие интерпретаторы без надлежащей проверки | |
| Наименование уязвимости | Протестировано | Проэксплуатировано |
| Accessing the file system | ДА | НЕТ |
| Code injection | ДА | ДА |
| Command injection | ДА | НЕТ |
| Format string injection | ДА | НЕТ |
| IMAP/SMTP injection | НЕТ | ДА |
| LDAP injection | НЕТ | НЕТ |
| ORM injection | НЕТ | НЕТ |
| Overflowing character buffers | ДА | ДА |
| Path traversal | ДА | НЕТ |
| SQL injection | ДА | ДА |
| SSI injection | ДА | НЕТ |
| XML injection | ДА | ДА |
| XPath injection | ДА | НЕТ |

Разработанная методика тестирования на проникновение была применена на реальных проектах по аудиту информационной безопасности зарубежной организации. В связи с соглашением о неразглашении, данные, раскрывающие информацию о клиенте, не приводятся.

## *Выводы*

Предложены следующие рекомендации по улучшению существующих методик проведения тестирования на проникновение:

- стабильное обновление методики раз в квартал – информационные технологии развиваются стремительно, необходимо всегда следовать актуальным трендам в области защиты информации;
- немедленное обновление методики при обнародовании новой уязвимости;
- постоянное информирование сотрудников о новых уязвимостях в виде статей на внутреннем ресурсе компании – исследователям требуется каждый день повышать свою квалификацию, а также делиться знаниями между собой;
- назначение ряда ответственных лиц – в компании следует уделять повышенное внимание вопросу актуальности используемой методики;
- регулярные обсуждения внутри компании на предмет актуальности используемой методики, исключение устаревших или добавление недавно опубликованных уязвимостей;
- анализ проведенной работы, доработка шаблонов и написание документации для новых сотрудников.

## *Заключение*

В работе изучены особенности проведения тестирования на проникновение, проведен сравнительный анализ существующих методик тестирования на проникновение, разработана методика тестирования на проникновение мобильных и веб-приложений, и предложены рекомендации по улучшению качества существующих методик тестирования на проникновение.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Pentest (penetrationtesting) [Электронный ресурс] / отдел «Penetrationtesting». – Электрон. дан. – СФ., 2018. – Режимдоступа: https://searchsecurity.techtarget.com/definition/penetration-testing. – Загл. с экрана.

2. Importance Of Information Security In Organizations Information Technology Essay [Электронный ресурс] / отдел « Information Technology». – Электрон. дан. – К., 2011. – Режим доступа: https://www.uniassignment.com/essay-samples/information-technology/. – Загл. сэкрана.

3. Introduction: Intelligence Gathering & Its Relationship to the Penetration Testing Process [Электронный ресурс] / отдел «Penetration testing». – Электрон. дан. – НЙ., 2016. – Режим доступа: https://resources.infosecinstitute.com/penetration-testing-intelligence-gathering/. – Загл. сэкрана.

4. Technical Guideto Information Security Testingand Assessment [Электронный ресурс] / отдел «Publications». – Электрон. дан. – МД., 2008. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. – Загл. с экрана.

5. Introduction to Penetration Testing and Kali Linux. [Электронный ресурс] / отдел «Security» – Электрон. дан. – Б, 2015. – Режим доступа: https://hub.packtpub.com/introduction-penetration-testing-and-kali-linux/. – Загл. с экрана.

6. Exploit database. Exploits for web applications. [Электронный ресурс] / отдел «Exploits» – Электрон. дан. – НЙ, 2016. – Режим доступа: https://www.exploit-db.com/webapps. – Загл. с экрана.

7. Payment application data security standard. Requirements and security assessment procedures. Version 3.1. Payment Card Industry (PCI). [Электронный ресурс] / отдел «Стандарты PCI-DSS» – Электрон. дан. – НЙ, 2017. – Режим доступа: https://www.pcisecuritystandards.org/documents/PADSS_v3-1.pdf. – Загл. с экрана.

8. TheOpen Source Security Testing Methodology Manual [Электронныйресурс] / отдел «Research». – Электрон. дан. – НЙ., 2010. – Режим доступа: http://www.isecom.org/mirror/OSSTMM.3.pdf. – Загл. с экрана.

9. Mitnick, Kevin. Unauthorized Access: Physical Penetration Testing for IT Security Teams [Текст] – НЙ.: John Wiley & Sons, 2009. – 287 с.

10. MobileTop 10 2016-Top 10 [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2016. – Режим доступа: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10. – Загл. с экрана.

11. OWASP Mobile Security Testing Guide [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2018. – Режим доступа: https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide. – Загл. с экрана.

12. OWASP Testing Guide v4 [Электронный ресурс] / отдел «Publications». – Электрон. дан. – ЛА., 2014. – Режим доступа: https://www.owasp.org/images/1/19/OTGv4.pdf. – Загл. с экрана.

13. OWASP Top Ten Project [Электронный ресурс] / отдел «Projects». – Электрон. дан. – ЛА., 2017. – Режим доступа: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. – Загл. с экрана.

14. Testing Guide Introduction [Электронный ресурс] / отдел «Projects». – Электрон.дан. – ЛА., 2014. – Режим доступа: https://www.owasp.org/index.php/Testing_Guide_Introduction. – Загл. с экрана.

15. Vacca, John R. Computer and Information Security Handbook [Текст] – ЛА.: Elsevier, 2017. – 1280 с.

16. Black box, grey box, white box testing: what differences? [Электронный ресурс] / отдел «Blog». – Электрон. дан. – П., 2016. – Режим доступа: https://nbs-system.com/en/blog/black-box-grey-box-white-box-testing-what-differences/. – Загл. с экрана.

17. ARP Spoofing [Электронный ресурс] / отдел «Security». – Электрон. дан. – НЙ., 2016. – Режим доступа: https://www.veracode.com/security/arp-spoofing/. – Загл. с экрана.

18. What is MAC Flooding? How to prevent it? [Электронный ресурс] / отдел «KB». – Электрон.дан. – ЛА., 2015. – Режим доступа: https://www.interserver.net/tips/kb/mac-flooding-prevent/. – Загл. с экрана.

19. Microsoft Security Development Lifecycle. [Электронный ресурс] / отдел «Безопасный цикл разработки Microsoft» – Электрон.дан. – СФ, 2016. – Режим доступа: http://www.microsoft.com/security/sdl/default.aspx. – Загл. с экрана.

20. XPathinjection. [Электронный ресурс] / отдел «IssueDefinitions» – Электрон.дан. – ЛА, 2018. – Режим доступа: https://portswigger.net/kb/issues/00100600_xpath-injection. – Загл. с экрана.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-54-60

# О ВЫБОРЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

***Алина Павловна Жумаева***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (999)466-04-55, e-mail: zhumaevanalina@gmail.ru

***Валентина Андреевна Ялбаева***
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, бакалавр информационной безопасности, тел. (960)975-49-15, e-mail: valya_599@mail.ru

***Полина Александровна Звягинцева***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

***Валентин Валерьевич Селифанов***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: sfo1@mail.ru

В статье рассматривается проблема выбора средств защиты информации в государственной информационной системе, а именно межсетевые экраны и средства обнаружения вторжений. Данная проблема актуальна, так как в последние годы обеспечение информационной безопасности, как никогда, востребовано.

**Ключевые слова:** межсетевой экран, средства обнаружения вторжения, программное обеспечение, информационная система, средство защиты информации, сетевая атака, уровень защиты информации, недекларированные возможности, сервер.

# CHOICE OF MEANS OF INFORMATION SECURITY FOR GOVERNMENT INFORMATION SYSTEMS

***Alina P. Zhumaeva***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Bachelor of Information Security, phone: (999)466-04-55

***Valentina A.Yalbaeva***
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Bachelor of Information Security, phone: (960)975-49-15

***Polina A. Zviagintcheva***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: p.a.zvjaginceva@sgugit.ru

***Valentin V. Selifanov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: sfo1@mail.ru

The article deals with the problem of choosing the means of information security in the state information system, namely firewalls and intrusion detection. The problem is relevant since information security is in demand more than ever.

**Key words:** firewall, intrusion detection system, software, information system, information security tool, network attack, information security level, undeclared capabilities, server.

Начиная с 2011 года, начался процесс изменения требований к средствам защиты информации. Осуществляется переход на систему требований нового поколения, основанную на международной серии стандартов ИСО/МЭК 15408 или «общие критерии». Все большее значение приобретают средства обеспечения безопасности межсетевого взаимодействия. Однако стоит рассмотреть комплексное решение.

После изменений требований все средства защиты информации (СЗИ) от несанкционированного доступа (НСД) классифицируются по видам, классам и типам.

Под видом СЗИ понимается конкретное средство, которое используется. Это может быть:

– антивирусное СЗИ, которое должно выявлять и соответствующим образом реагировать на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ;

– межсетевые экраны – средства, реализующие контроль за информацией, направленной в автоматизированную систему или исходящей из нее. Межсетевые экраны выполняют фильтрацию информации по заданным критериям;

– средство доверенной загрузки – программно-технические средства, которые реализуют функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки;

– система обнаружения вторжений (СОВ, соответствующий английский термин Intrusion Detection System (IDS)– программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть, либо несанкционированного управления ими в основном через Интернет.

Каждому виду соответствует 6 классов, которые зависят от уровня защищаемой информации (1–3 это государственная тайна, 4–6 иная информация ограниченного доступа и т. д.). В данной работе будут рассмотрены СЗИ 4–6 классов.

Кроме вида и класса средства защиты, выделяется тип СЗИ – где применяется это средство защиты информации и что оно делает.

Проблема выбора СЗИ в ГИС.

Защита информационной системы нуждается не только в выборе средства защиты информации, но еще и выполнении ряда определенных требований, а также проведении оценки эффективности [8–10].

В соответствии с приказом ФСТЭК России № 17от 11 февраля 2013 г п. 26, для проектирования системы защиты информационной системы необходимо:

– определить типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

– определить методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

– выбрать меры защиты информации, подлежащие реализации в системе защиты информации информационной системы [11];

– определить виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определить структуру системы защиты информации, информационной системы, включая состав (количество) и места размещения ее элементов;

– осуществить выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

– определить требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

– определить меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Как правило, часть угроз можно нейтрализовать, используя волоконно-оптические линии связи, однако ограничиваться этим нельзя и необходимо выбирать виды систем защиты информационной системы исходя из актуальных угроз [7]. Серьезное внимание стоит уделить типам и классам. Сузим область и рассмотрим не все виды средств защиты, а лишь некоторые из них – межсетевые экраны и системы обнаружения вторжений и такой вид информационной системы как ГИС.

Классы защиты определяются в соответствии с нормативными правовыми актами ФСТЭК России.

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом:

– в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса;

– в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса;

– в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса.

Если посмотреть на оборудование Cisco (Cisco – американская компания, разрабатывающая и продающая сетевое оборудование, предназначенное в основном для крупных организаций и телекоммуникационных предприятий), в нем присутствует много межсетевых экранов, соответствующих 5 классу защиты для межсетевых экранов [4], при этом контроль отсутствия недекларированных возможностей не проводился. Таким образом использовать рассматриваемые средства в системе защиты информации ГИС 1 и 2 класса защиты, а так же информационных систем персональных данных 1, 2 и частично 3 уровня защищенности нельзя [3].

Обратимся к типам межсетевых экранов. Требованиями Информационного сообщения ФСТЭК от 28 апреля 2016 г. № 240/24/1986, выделены 5 типов межсетевых экранов:

– уровня сети (тип «А») – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;

– уровня логических границ сети (тип «Б») – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы;

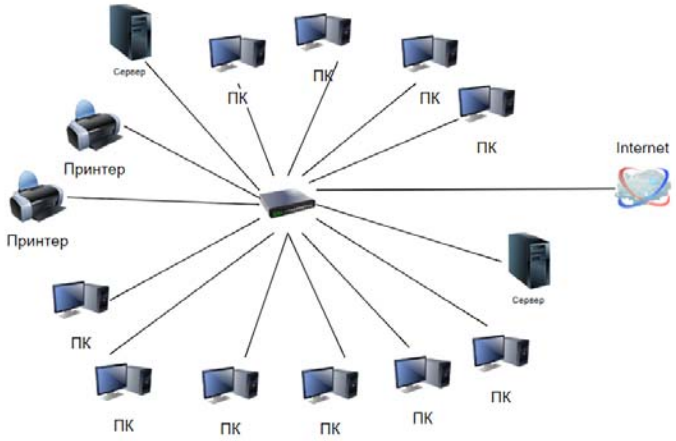
– уровня узла (тип «В») – межсетевой экран, применяемый на узле (хосте) информационной системы;

– уровня веб-сервера (тип «Г») – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера);

– уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Если рассмотреть небольшие государственные информационные системы (до 20 автоматизированных рабочих мест – это рабочее место интерпретатора, оборудованное персональным компьютером с периферийными устройствами, для автоматизированной обработки и интерпретации материалов, а также выдачи результатов), то можно наблюдать, что пользователи выбирают исключи-

тельно программные межсетевые экраны, так как для их использования достаточно установить лишь специальное программное обеспечение. Обычно организация с трудом может найти компьютер, отвечающий всем техническим требованиям, зачастую довольно высоким.




Топология сети

Разберем данную проблему на примере сети, состоящей из 2 серверов, 2 сетевых принтеров, 10 рабочих мест, и одного коммутатора (рис.1). Даже если на свой домашний компьютер поставить персональный межсетевой экран (межсетевой экран типа «В» может иметь только программное исполнение), можно увидеть, что при таком простом коммутируемом подключении к Интернет с динамически выделяемым IP-адресом он подвергается, по крайней мере, одной сетевой атаке (например: вирусы, троянские программы, распространение сетевого червя, логические бомбы, эксплойты, бот сети, руткиты, фишинг, фарминг) каждые несколько часов работы в сети. А в нашем случае это сеть, состоящая из 10 рабочих станций. Можно сделать вывод о том, насколько интенсивное давление испытывает эта информационная система. А ущерб от любой из этих атак на сеть может многократно превысить не только стоимость системы безопасности, но и всей информационной сети.

Именно поэтому крупные компании предпочитают установку специализированных программно-аппаратных комплексов (межсетевые экраны типа «А»), получивших название «security appliance». Работают они чаще всего на основе систем Linux.

Такое решение имеет следующие преимущества:

– легкое и простое управление: контроль работы программно-аппаратного комплекса осуществляется с любого стандартного протокола (Telnet, SNMP) – или защищенного (SSL, SSH);

– высокая производительность: работа операционной системы направлена на одну единственную функцию, из нее исключены любые посторонние сервисы;

– отказоустойчивость: программно-аппаратные комплексы эффективно выполняют свою задачу, вероятность сбоя практически исключена.

Данная проблема касается всех: ситуация, когда работа с сервером осуществляется через веб-браузер, но ни межсетевого экрана типа «Г», ни системы обнаружения вторжений нет. Система обнаружения вторжений и межсетевой экран не позволяют злоумышленникам воздействовать на информационную систему посредством сетевых атак. Но отличаются они тем, что межсетевой экран ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети, а СОВ пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. В данном случае опасен как внутренний, так и внешний нарушитель, потому что есть возможность подключения к Интернету. В этом случае злоумышленник может реализовать атаки:

- взлом паролей;
- отключение/обход систем аудита;
- использование снифферов и sweepers (систем контроля содержимого);
- использование программ диагностики сети для получения необходимых данных;
- подмена данных в IP-пакетах;
- атаки типа «отказ в обслуживании» (DoS);
- атаки на Web-серверы (CGI-скрипты).

Во избежание вышеперечисленных проблем рекомендуется устанавливать комплексную защиту, включающую в себя такие средства защиты информации как межсетевые экраны типа «А», «Г» (SecretNet Studio) и систему обнаружения вторжений (Security Studio Endpoint Protection).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационное письмо ФСТЭК России об утверждении требований к системам обнаружения вторжений.

2. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.

3. Приказ 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Информационное сообщение ФСТЭК России об утверждении требований к межсетевым экранам от 28 апреля 2016 г. N 240/24/1986.

5. Информационное сообщение ФСТЭК России об утверждении методических документов, содержащих профили защиты межсетевых экранов от 12 сентября 2016 г. N 240/24/4278.

6. Информационное сообщение ФСТЭК России по вопросам разработки, производства, поставки и применения межсетевых экранов, сертифицированных ФСТЭК России по требованиям безопасности информации от 24 марта 2017 г. N 240/24/1382.

7. Селифанов В.В., Звягинцева П.А., Юракова Я.Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

8. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. С. 109-113.

9. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 220–225.

10. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов, Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015, стр. 208-213

11. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. 2014. № 23. С. 188.

УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-61-65

# ПРИМЕНЕНИЕ SIEM РЕШЕНИЙ НА МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

***Глеб Владимирович Попков***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности; Сибирский государственный университет телекоммуникаций и информатики, 630009, Россия, г. Новосибирск, ул. Гурьевская, 9, доцент кафедры безопасности и управления в телекоммуникациях, тел. (383)343-91-11, e-mail: glebpopov@inbox.ru

В статье рассмотрены решения в области систем управления инцидентами безопасности SIEM (Security information and event management) и работа систем обнаружения / предупреждения сетевых вторжения класса IDS/IPS. Приводятся общие функциональные характеристики данных программных продуктов, предлагаются типовые решения по включению IDS/IPS в сеть передачи данных, на втором и третьем, четвёртом уровне модели OSI. Даётся краткое описание и некоторые практические примеры по применению IDS/IPS компании Sourcefire, продукта SNORT.

**Ключевые слова:** защита информации, SIEM, СОВ, IDS/IPS, SNORT.

# APPLICATION OF SIEM SOLUTIONS ON MULTI-SERVICE COMMUNICATIONS NETWORKS

***Gleb V. Popkov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security; Siberian State University of Telecommunications and Informatics, 9, Gurievskaya St., Novosibirsk, Russia, 630009, Associate Professor, Department of Security and Management in Telecommunications, phone: (383)343-91-11, e-mail: glebpopov@inbox.ru

The article discusses solutions in the field of SIEM (Security information and event management systems) and the operation of IDS / IPS class network intrusion detection / prevention systems. The general functional characteristics of these software products are presented, typical solutions for the inclusion of IDS / IPS in data transmission network are offered, at the second, third and fourth levels of the OSI model. A brief description and some practical examples of using IDS / IPS from Sourcefire, the SNORT product, are given.

**Key words:** information security, IDS/IPS, SNORT.

Традиционное применение межсетевых экранов для фильтрации трафика сетей передачи данных зачастую недостаточно для обнаружения сетевых атак на канальном, сетевом и транспортном уровнях модели OSI.

Широко распространенные системы обнаружения и предотвращения вторжений IDS/IPS (анг. Intrusion detection system/Intrusion prevention system) и их дальнейшее развитие системы класса NGIPS обеспечивают приемлемые решения для мониторинга и локализации сетевых аномалий. Данные решения входят в более обширный класс систем предупреждения инцидентов безопасности SIEM.

К основному функционалу SIEM систем относится:

- сбор, обработка, анализ инцидентов безопасности;
- анализ рисков безопасности;
- принятие эффективных методов по защите информации;
- обнаружение аномалий сетевого трафика, возможных вторжений;
- прогнозирование и поиск возможных уязвимостей;
- выявление возможного источника атаки;
- формирование онтологий событий сетевых вторжений;
- формирование принципов администрирования сетевого оборудования.

В отличие от сетевых экранов указанные системы могут просматривать содержимое пакетов, что повышает возможности системы обнаруживать «аномальные» пакеты. Принятие решения о пропуске или блокировке пакета ложится, в данном случае, на подсистему SIEM IDS/IPS. В таких системах очень важно задание правил сканирования входящего трафика. В случае большого количества ограничений на сканируемые пакеты, возможен рост ложных срабатываний, на предмет получения «аномальных» пакетов данных, что приводит к большому количеству формируемых алармистских сообщений администраторам сети, это ведёт к непроизводительной работе системы.

Очевидно, что формирование правил облегчающих или упрощающих прохождение нежелательных пакетов приводит к повышению вероятности проведения успешной атаки нарушителем. Как правило, операторы пакетных сетей передачи данных используют систему IDS/IPS в двух основных режимах работы. Первый режим характеризуется постоянным сканированием в реальном режиме времени поступающего трафика на сетевое оборудование, второй режим является инцидентным, в зависимости от поведения поступающего трафика формируются решения от системы IDS/IPS по изменению политики пропуска поступающего трафика в защищаемую сеть.

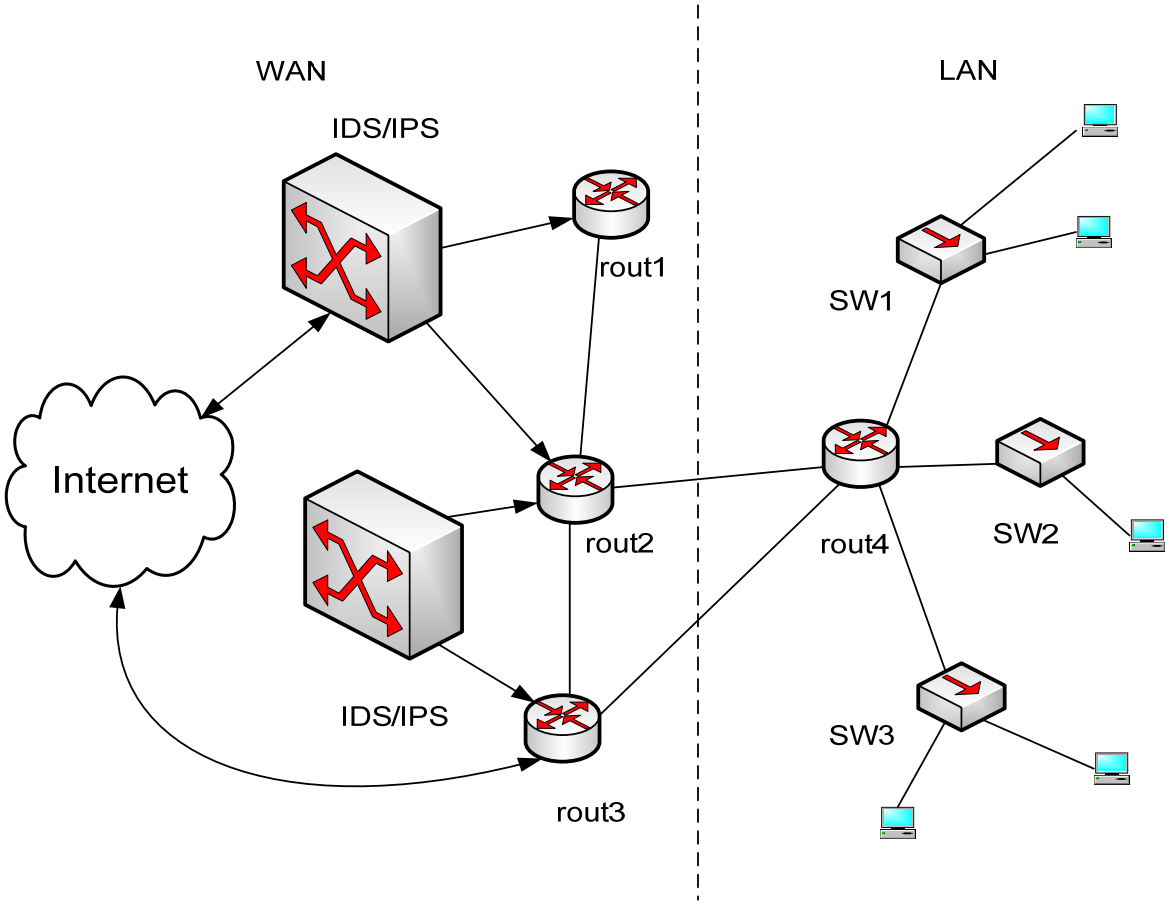
Возможны, два типа подключения IDS/IPS к действующему сетевому оборудованию, модули IDS/IPS ставятся между внешними сетями и защищаемой сетью, второй вариант – модули работают параллельно портам сетевого оборудования обслуживающего поступающий трафик в защищаемую сеть.

Дальнейшее развитие этих программных сенсоров получили системы NGIPS (англ. Next generation intrusion prevention system), преимуществом этой генерации платформ является, эффективная работа онлайн, наименьшим образом влияющая на скорость обработки данных. Использование единой платформы и децентрализованного управления позволяют выполнять контроль критически важных приложений и их мониторинг. NGIPS эффективно анализирует содержимое файлов, имеют возможность использовать внешние источники по базам уязвимостей (base vulnerability), а также использовать данные геолокации. В сетевой инфраструктуре IPS модули новой генерации могут использоваться в режиме IDS, например, анализируя поступающий трафик со SPAN портов маршрутизаторов, или используя технологию Network Tap.

Системы NGIPS имеют возможность поддержки протокола STP, способны маршрутизировать трафик по протоколам RIP, OSPF. NGIPS имеют возмож-

ность строить карту сети используя информацию со SPAN-портов, а также производят активное сканирование оборудования.

Приведём пример типового включения оборудования IDS/IPS в сети передачи данных, рисунок.




Пример типового включения IDS\IPS

Одним из самых популярных программных решений IDS/IPS является ПО Snort, это GNU/GPL программное обеспечение с открытым исходным кодом поддерживается компанией Sourcefire (входит в состав Cisco inc.).

Основные возможности Snort IDS/IPS:

– анализ трафика согласно правилам, установленным администратором защищаемой сети;

– использование эксплойтов (Shellcode);

– сканирование портов активного сетевого оборудования, операционных систем, пользователей сети;

– возможность определения атаки на WEB- сервисы;

– блокирование DoS/DDoS атак;

– возможность выявления атак на базы данных SQL, Oracle и. т. д;

– возможность WEB-фильтрации;

– блокирование атак по протоколам SNMP, NetBios, SMTP, ICMP и т.д.

В различных режимах работы Snort может блокировать трафик, анализировать трафик согласно правилам, вести журналирование, скрывать IP- адреса, выдавать ALERT -сообщения согласно ранее прописанным правилам администратора защищаемой сети. Возможности расширенных версий Snort позволяют создавать такие пользовательские конфигурации, которые полностью контролируют весь трафик, циркулирующий в сети передачи данных.

Например, в режиме анализа пакетов Snort просто читает пакеты, приходящие из сети, и выводит их на экран монитора администратора. Если ставится задача вывести на экран заголовки пакетов TCP/IP, необходимо прописать команду snort –v. Эта команда выводит заголовки IP и TCP, UDP, ICMP пакетов. Если есть потребность, кроме того, увидеть данные, содержащиеся в пакетах, используется команда: snort -vd. Для еще более подробного вывода, включающего заголовки кадров канального уровня, используется команда snort -vde.

Пример выводимой информация представлен ниже.

```
01/18-15:06:17.807867 0:E0:81:2F:FE:2C ->0:0:C:7:AC:2 type:0x800
len:0x5EA
66.179.164.20:22 ->24.136.161.188:62456 TCP TTL:64 TOS:0x10 ID:27401
IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x50692152 Ack: 0xDD1E2B42 Win: 0x2180 TcpLen: 20
AA A8 5A 92 A7 BF DF 32 7D BF F7 7B 1B 5C 35 47
..Z....2}..{.\5G...mhA.S+....1B E0 C9 87 A8 71 91 EA D0 F4 1C 6C B4…
```

Система Snort анализирует трафик до тех пор, пока не поступит комбинация клавиш завершения захвата пакетов Ctrl-C. После нажатия Ctrl-C выводится отчёт о захваченных пакетах. Пример отчёта показан далее.

```
Snort received 74260 packets
Analyzed: 5923(7.976%)
Dropped: 68337(92.024%)
Breakdown by protocol:
TCP: 1602 (2.157%)
UDP: 4142 (5.578%)
ICMP: 0 (0.000%)
ARP: 6 (0.008%)
EAPOL: 0 (0.000%)
IPv6: 0 (0.000%)
IPX: 0 (0.000%)
ALERTS: 0
LOGGED: 0
PASSED: 0
Snort exiting
```

В версии Snort 2.3.0 RC1 интегрирована новая возможность, предупреждения вторжений (Intrusion Prevention System, IPS) snort_inline. Snort_inline получает пакеты не от libpcap, а от iptables, и с помощью новых типов правил помогает определить, что нужно сделать с пакетом – пропустить или уничтожить. Этот режим Snort называется встраиваемым.

Теоретически количество правил, задаваемых для систем подобных Snort, может быть неограниченное количество, определяемое администрацией сети связи. На практике количество правил ограничивается готовыми шаблонами известных атак, прописанных в онтологиях баз данных систем IDC/IPS.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бирюков А. А. Информационная безопасность: защита и нападение. – 2-е изд. – М. : ДМК Пресс, 2017. – 434 с. – ISBN 978-5-97060-435-9. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/93278.

2. Шаньгин В. Ф. Защита компьютерной информации : учеб. пособие. – М. : ДМК Пресс, 2010. – 544 с. – ISBN 978-5-94074-518-1. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/1122.

3. Snort [Электронный ресурс] / отдел «Documents». – Электрон. дан. – ЛА., 2019. – Режим доступа: https://www.snort.org/documents. – Загл. с экрана.

УДК 621.396.67
DOI: 10.33764/2618-981X-2019-9-66-71

# МОДЕЛИРОВАНИЕ ПЛАЗМОННОГО ОДИНОЧНОГО ГРАФЕНОВОГО ОТРАЖАТЕЛЬНОГО МОДУЛЯ ТЕРАГЕРЦОВОГО ДИАПАЗОНА

***Александр Григорьевич Черевко***
Сибирский государственный университет телекоммуникации и информатики, 630106, Россия, г. Новосибирск, ул. Кирова, 86, кандидат физико-математических наук, доцент, зав. кафедрой физики, e-mail: cherevko@mail.ru

***Юрий Вячеславович Моргачев***
Сибирский государственный университет телекоммуникации и информатики, 630106, Россия, г. Новосибирск, ул. Кирова, 86, инженер, e-mail: morgachev.yury@gmail.com

В статье представлены результаты моделирования плазмонного одиночного графенового отражательного модуля, работающего на частоте 1,35 ТГц. Рассмотрены зависимости характеристик плазмонного одиночного графенового отражательного модуля от изменения различных параметров графена (температура, химический потенциал и время релаксации).

**Ключевые слова:** ТГц, терагерцовый, графен, антенна, отражательная антенная решетка, плазмон.

# TERAHERTZ GRAPHENE PLASMON SINGLE REFLECTARRAY MODULE MODELING

***Alexander G. Cherevko***
Siberian State University of Telecommunications and Informatics, 86, Kirova St., Novosibirsk, 630106, Russia, Ph. D., Associate Professor, Head of Physics Department, e-mail: cherevko@mail.ru

***Yury V. Morgachev***
Siberian State University of Telecommunications and Informatics, 86, Kirova St., Novosibirsk, 630106, Russia, Engineer, e-mail: morgachev.yury@gmail.com

Simulation of a plasmon single graphene reflectarray module operating at a frequency of 1.35 THz is presented. The dependences of the characteristics of a plasmon single graphene reflectarray module on changes in various parameters of graphene (temperature, chemical potential and relaxation time) are considered.

**Key words:** THz, terahertz, graphene, antenna, reflectarray, plasmon.

## *Введение*

Приёмники и излучатели ТГц диапазона (300 ГГц – 10 ТГц) нашли широкое применение в таких областях как получение изображений скрытых предметов под одеждой [1], радиоастрономия [2], медицина [3], передача данных [4]. Из-за высокого атмосферного поглощения ТГц излучения, одним из требований к приемо-передающим устройствам является наличие высоконаправленной антенны [5]. Для многих приложений существенную роль играют габариты ан-

тенны. Отражательные антенные решетки (ОАР) позволяют выполнить эти требования. ОАР реализуют достоинства зеркальных антенн и фазированных антенных решеток, поэтому их применение в ТГц области изучается достаточно активно [6-8]. Они обладают низкими потерями, планарным дизайном, низким уровнем кросс поляризации, простотой изготовления и высокой эффективностью. ОАР состоит из набора отражательных модулей (рис. 1), которые вводят фазовый сдвиг при отражении падающей волны. Облучение же производится отдельно расположенным источником, по аналогии с зеркальной антенной, например, рупорной антенной. В зависимости от распределения фазы на поверхности ОАР, возможно изменять форму диаграммы направленности.

Рис. 1. 48 элементная ОАР с первичным облучателем

Одним из перспективных материалов, применимых при конструировании ТГц ОАР является графен. Графен имеет высокую подвижность носителей заряда и чувствительность к внешнему электрическому полю, из-за чего активно применяется в электронике. При рассмотрении пассивных устройств, например, антенн, интерес к графену основывается на его комплексной поверхностной проводимости, которая позволяет распространяться медленным плазмонным модам. Использование данного эффекта позволяет уменьшать размеры ОАР на 2 порядка [9].

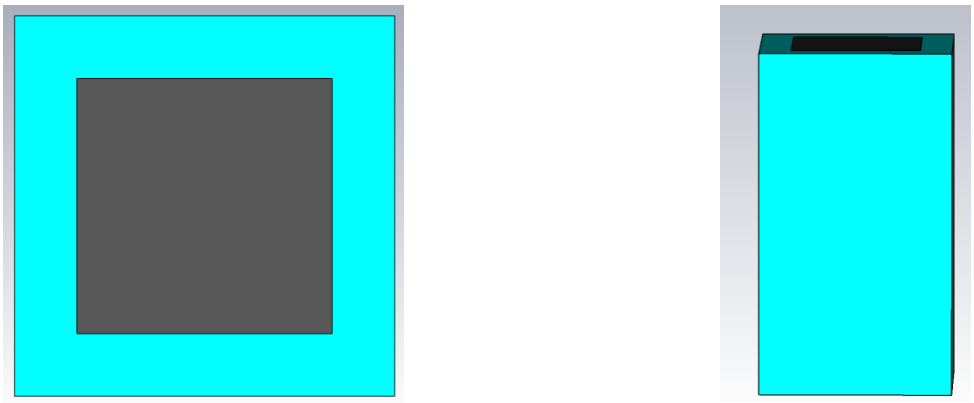
Целью данной работы является исследование зависимости характеристик плазмонного одиночного графенового отражательного модуля от изменения различных параметров графена, таких как химический потенциал, температура и время релаксации.

## *Методы и материалы*

Для достижения поставленной цели разработана компьютерная плазмонного графенового одиночного отражательного модуля (ПГООМ) для чего использовался программный пакет CST Studio. Посредством решателя в частотной области получены характеристики ПГООМ. В качестве граничных условий

использовались граничные условия Флоке. С обратной стороны ПГООМ находится заземляющая пластина, поэтому устанавливается соответствующие граничные условия (Et = 0). Данная конфигурация позволяет учесть межэлементную связь и варьировать углы падения волны.

Дизайн плазмонного графенового одиночного отражательного модуля представлен на рис. 2. Графеновый полосок представляет из себя квадрат, со сторонами длиной ~$\lambda_0/24$.



*а*) вид сверху *б*) вид сбоку

Рис. 2. Дизайн ПГООМ

В качестве материала подложки использовался кварц (бирюзовый цвет) (диэлектрическая проницаемость 3,75 и тангенс угла потерь 0,0184 в ТГц диапазоне) толщиной h = 24 мкм. Длина и ширина ПГООМ составляет 15 мкм. Из-за толщины слоя графена в 1 атом, данный слой может быть представлен как бесконечно тонкая поверхность с комплексной проводимостью. Данная проводимость может быть получена с помощью формулы Кубо. В качестве параметров использовались: температура 293 К, время релаксации 1 пс (измерено в [10]), химический потенциал 0,19 эВ, по аналогии с [11].

## *Результаты и их обсуждение*

Полученная комплексная проводимость представлена на рис. 3.

Рабочая частота ПГООМ равна 1,35 ТГц, лежит в окне пропускания атмосферы [12] и используется в спектроскопии. Полученный размер полоска после оптимизации составляет 9,2 мкм.

Как видно из рис. 4, существенное влияние на амплитуду и фазу коэффициента отражения ПГООМ оказывает изменения химического потенциала графена.

Можно заметить, что резонансная кривая (рис. 4, слева) на 0,2 эВ не сохраняется при изменении химического потенциала. На рис. 4 (справа) можно заметить, что фазу отраженного сигнала можно варьировать с помощью изменения постоянного внешнего электрического поля, что подтверждает результаты [13].

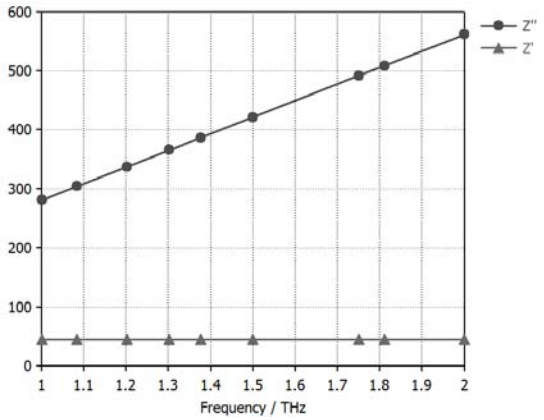



Рис. 3. Комплексная проводимость графеная, в диапазоне от 1 до 2 ТГц

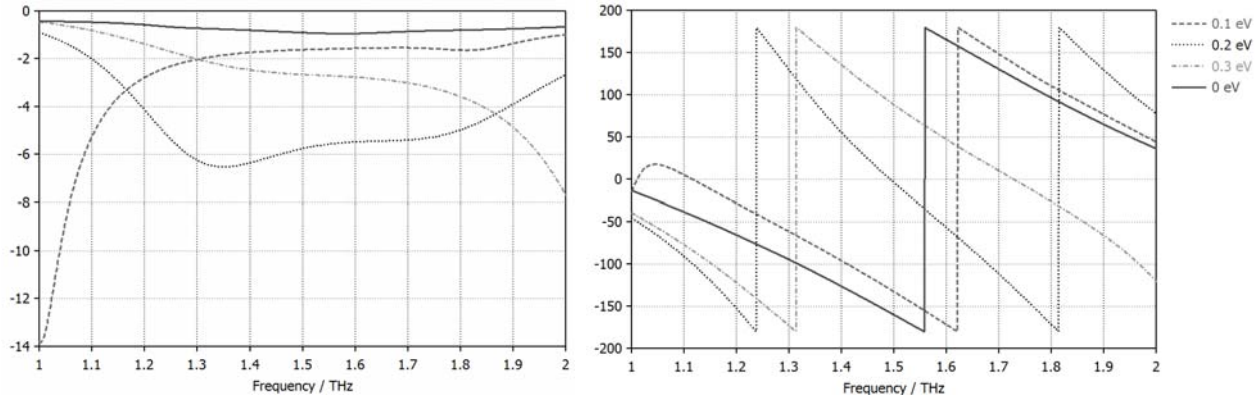



Рис. 4 Влияние химического потенциала на коэффициент отражения ПГООМ, слева: амплитудно-частотная характеристика, справа: фазо-частотная характеристика

Влияние изменения времени релаксации на амплитуду и фазу коэффициента отражения представлено на рис. 5.

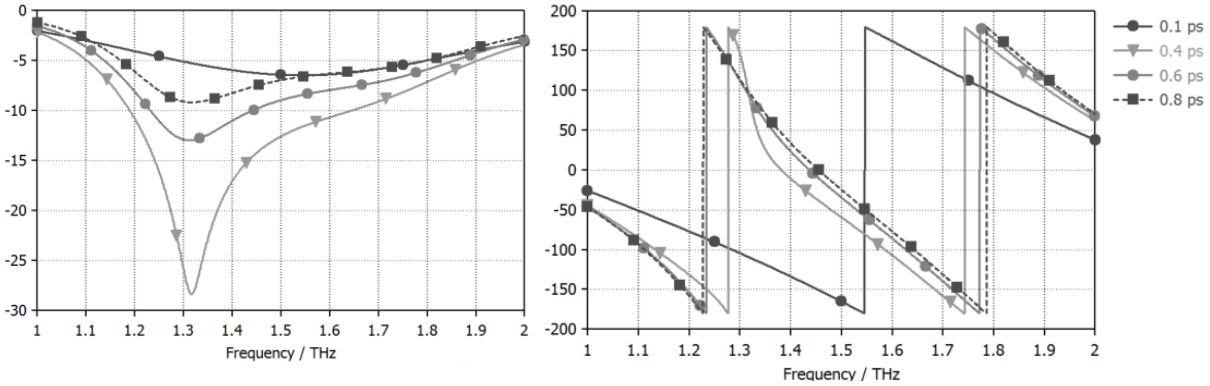



Рис. 5. Влияние времени релаксации электрона на коэффициент отражения ПГООМ. Слева: АЧХ, справа: ФЧХ

Получено, что изменение времени релаксации плавно меняет резонансный характер АЧХ (рис. 5 слева), в отличии от химического потенциала (рис. 4, слева). Устойчивая фаза отраженного сигнала устанавливается после значений времени релаксации в 0,5 пс (рис. 5, справа).

Отражательные антенные решетки должны работать в различных температурных режимах, поэтому целесообразно рассмотреть влияние температуры на коэффициент отражения ПГООМ (рис. 6).

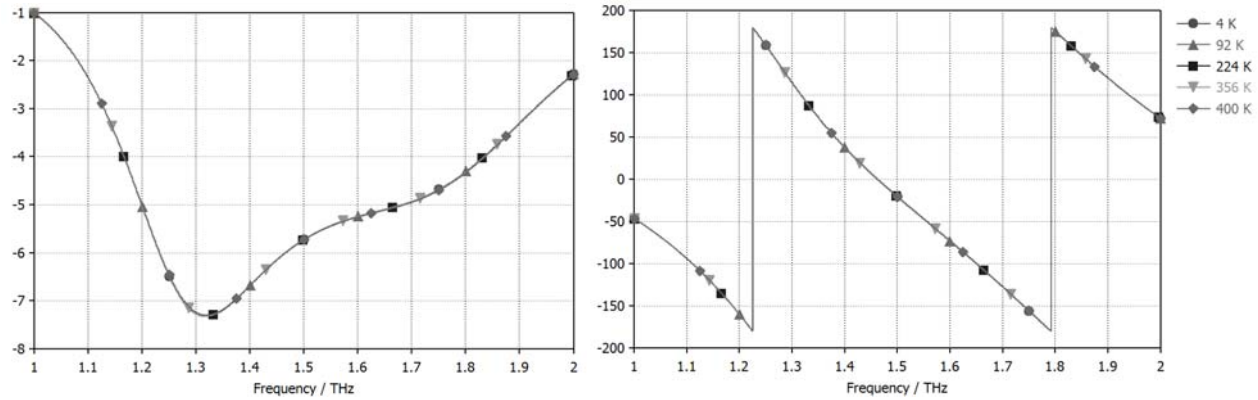



Рис. 6. Влияние температуры на коэффициент отражения ПГООМ.
Слева: АЧХ, справа: ФЧХ

Как видно из рис. 6, изменение температурного режима не влияет на результирующие параметры ОАР (точки, соответствующие разным температурам, ложатся на одну и туже) кривую.

## *Заключение*

Результаты моделирования показали: что на плазмонную графеновую отражательную антенную решетку серьезное влияние оказывает внешнее электрическое поле, которое изменяет химический потенциал графена, т.е. необходима стабилизация ОАР по этому параметру. В тоже время ОАР индифферентна к изменению ее температурного режима.

Время релаксации электронов в графене зависит напрямую от выбранной технологии изготовления графеновых полосков, что так же должно быть принято во внимания при моделировании ПГООМ и соответственно ОАР.

### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Kemp M.C. и др. Security applications of terahertz technology // Terahertz for Military and Security Applications. 2003. С. 44–52.

2. Shi S. Development of superconducting mixers for THz astronomy // Science China Information Sciences. 2011. Т. 55. № 1. С. 120–126.

3. Sun Q. и др. Recent advances in terahertz technology for biomedical applications // Quantitative Imaging in Medicine and Surgery. 2017. Т. 7. № 3. С. 345–355.

4. Akyildiz I.F., Jornet J.M., Han C. Terahertz band: Next frontier for wireless communications // Physical Communication. 2014. Т. 12. С. 16–32.

5. Tamosiunaite M. и др. Atmospheric Attenuation of the Terahertz Wireless Networks // Broadband Communications Networks - Recent Advances and Lessons from Practice. 2018. С. 143–157.

6. Chang Z. и др. A Reconfigurable Graphene Reflectarray for Generation of Vortex THz Waves // IEEE Antennas and Wireless Propagation Letters. 2016. Т. 15. С. 1537–1540.

7. Frequencies: Design, Fabrication, and Measurement // IEEE Transactions on Terahertz Science and Technology. 2016. Т. 6. № 2. С. 268–277.

8. Miao Z.-W. и др. A 400-GHz High-Gain Quartz-Based Single Layered Folded Reflectarray Hasani H. и др. Tri-Band, Polarization-Independent Reflectarray at Terahertz

Antenna for Terahertz Applications // IEEE Transactions on Terahertz Science and Technology. 2019. Т. 9. № 1. С. 78–88.

9. Choudhury S.M. и др. Material platforms for optical metasurfaces // Nanophotonics. 2018. Т. 7. № 6. С. 959–987.

10. Mayorov A.S. и др. Micrometer-Scale Ballistic Transport in Encapsulated Graphene at Room Temperature // Nano Letters. 2011. Т. 11. № 6. С. 2396–2399.

11. Lee H., Paeng K., Kim I.S. A review of doping modulation in graphene // Synthetic Metals. 2018. Т. 244. С. 36–47.

12. Slocum D.M. и др. Atmospheric absorption of terahertz radiation and water vapor continuum effects // Journal of Quantitative Spectroscopy and Radiative Transfer. 2013. Т. 127. С. 49–63.

13. Carrasco E., Tamagnone M., Perruisseau-Carrier J. Tunable graphene reflective cells for THz reflectarrays and generalized law of reflection // Applied Physics Letters. 2013. Т. 102. № 10. С. 104103.

УДК 234.465+534.222
DOI: 10.33764/2618-981X-2019-9-72-76

# ОБОБЩЕННАЯ КИНЕТИКА ДЕТОНАЦИОННОГО СГОРАНИЯ ГАЗООБРАЗНЫХ УГЛЕВОДОРОДОВ

***Павел Аркадьевич Фомин***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат физико-математических наук, доцент кафедры специальных устройств, инноватики и метрологии; Институт гидродинамики им. М. А. Лаврентьева СО РАН, 630090, Россия, г. Новосибирск, пр. Академика Лаврентьева, 15, тел. (383)361-07-31, e-mail: kaf.suit@ssga.ru

Представлена двустадийная обобщенная модель химической кинетики детонационного сгорания углеводородов на примере пропилена. Первая стадия – период индукции, вторая – зона основного тепловыделения. Величина периода индукции полагается известной. Химические процессы во время периода индукции заменялись брутто-реакцией разложения пропилена. Модель физически обоснована, соответствует принципу Ле Шателье и второму началу термодинамики. Она проста (содержит лишь одно обыкновенное дифференциальное уравнение) и, соответственно, применима для численных неодномерных расчетов параметров и многофронтовой структуры детонационной волны.

**Ключевые слова:** газ, детонационное горение, химическая кинетика, обобщенная модель.

# GENERALIZED MODEL OF CHEMICAL KINETIC OF DETONATION COMBUSTION OF GASEOUS HYDROCARBONS

***Pavel A. Fomin***
Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Special Devices and Technologies; Lavrentiev Institute of Hydrodynamics SB RAS, 15, Prospect Akademik Lavrentiev St., Novosibirsk, 630090, Russia, phone: (383)361-07-31, e-mail: kaf.suit@ssga.ru

A two-step generalized model of chemical kinetics of detonation combustion of propylene is presented. The model is consistent with the second law of thermodynamics and Le Chatelier's principle. Constants of the models have a clear physical meaning. Owing to the simplicity (it includes only one ordinary differential equation) and high accuracy, the model can be used in multidimensional numerical calculations of detonation wave parameters and multi-front cellular structure.

**Key words:** gas, detonation combustion, chemical kinetic, generalized model.

Размер ячейки газовой детонации является важнейшим параметром, определяющим детонационные характеристики газовой смеси: геометрические и концентрационные пределы распространения детонационной волны и энергию его прямого инициирования [1]. Измерение размера детонационной ячейки не всегда возможно, особенно в случае больших (дороговизна и сложность эксперимента) и малых (низкая точность используемых методик) размеров ячеек. Поэтому численный расчет ячеистой структуры детонационной волны является

исключительно важной составной частью решения проблем взрывобезопасности газовых смесей.

Для численного расчета параметров и ячеистой структуры газовой детонации необходимо решить систему уравнений газовой динамики и химической кинетики. Детальные кинетические схемы химических превращений в углеводородо-кислородной смеси насчитывают сотни элементарных стадий. Поэтому их использование для расчетов неодномерной ячеистой структуры детонационной волны, как правило, невозможно, поскольку требует решения громоздкой жесткой системы обыкновенных дифференциальных уравнений и, соответственно, непреодолимых в настоящее время затрат машинного времени. Поэтому большое распространение в численном моделировании газовой детонации получили обобщенные кинетические модели, которые позволяют без решения детальной системы кинетических уравнений и нахождения точного химического состава газовой смеси, рассчитывать входящие в уравнения газовой динамики молярную массу и внутреннюю энергию газа.

Существующая практика обобщенного моделирования химических превращений в волне газовой детонации обладает рядом принципиальных недостатков. Рассматриваемые кинетические модели, как правило, не обладают высокой точностью, не соответствуют принципу Ле Шателье и второму началу термодинамики.

В нашей работе [2] предложена и апробирована обобщенная двустадийная модель кинетики детонационного сгорания метановых смесей. Она физически обоснована, соответствует принципу Ле Шателье и второму началу термодинамики. Модель проста (содержит лишь одно обыкновенное дифференциальное уравнение) и, соответственно, применима для численных неодномерных расчетов параметров и многофронтовой структуры детонационной волны. Использование данной модели позволило с высокой точностью рассчитать параметры и размер ячеистой структуры детонационной волны.

В настоящей работе предлагается обобщенная модель кинетики детонационного сгорания газообразного пропилена. Она будет основываться на обобщенной кинетической модели для метановых смесей [2]. Выбор пропилена в качестве объекта моделирования связан с его широким использованием в химической промышленности и, соответственно, большой вероятностью его утечки, смешении с воздухом и образованием облака пропилено-воздушной газовой смеси с последующей детонацией или взрывом. В качестве примера можно привести катастрофу, которая имела место в г. Гаосюн, Тайвань в 2014 году [3]. Тогда произошла утечка жидкого пропилена из заглубленного продуктопровода, проходящего через центр многомиллионного города. Произошло смешение испарившегося углеводорода с воздухом и распространение образовавшегося облака взрывчатой смеси по подземной дренажной системе сложной геометрии. Последовавший за этим взрыв унес жизни десятков людей и привел к масштабным разрушениям жилых и общественных зданий.

Рассматривается стехиометрическая смесь пропилена с воздухом: $C_3H_6 + 4{,}5(O_2 + 3{,}76N_2)$. Предлагаемая модель является двустадийной. Первая

стадия – период индукции, вторая – зона основного тепловыделения. Длительность периода индукции полагается известной.

Реальные многостадийные процессы, проходящие во время периода индукции, заменяются брутто-реакцией, которая удовлетворяет следующим условиям. (i) Рост температуры (и, соответственно, суммарное тепловыделение химических реакций) к моменту окончания периода индукции много меньше максимально возможного теплового эффекта, соответствующего полной рекомбинации продуктов реакции с образованием молекул $CO_2$ и $H_2O$. Выполнение этого условия гарантирует, что тепловой эффект брутто-реакции будет существенно меньше и теплового эффекта в плоскости Чепмена-Жуге детонационной волны. (ii) Во время периода индукции происходят химические реакции, связанные с появлением и ростом количества активных центров и развалом молекул углеводородного горючего. К моменту окончания периода индукции все молекулы углеводорода разлагаются. Исходя из условий (i), (ii) полагается, что каждая молекула пропилена в смеси во время периода индукции рано или поздно испытывает следующее химическое превращение:

$$C_3H_6 + 3O_2 \rightarrow 3CO + 3OH + 1{,}5H_2.$$

Если $\beta$ – доля молекул пропилена, еще не разложившихся к какому-то моменту времени $t$ внутри зоны индукции, то химический состав газовой смеси при этом имеет вид:

$$C_3H_6 + 4{,}5(O_2 + 3{,}76N_2) \rightarrow \beta C_3H_6 + (3\beta + 1{,}5)O_2 + (1 - \beta)3OH + (1 - \beta)1{,}5H_2 + 16{,}92N_2.$$

Если известна зависимость $\beta$ от времени, то последнее выражение позволяет рассчитать точный химический состав смеси во время периода индукции и, соответственно, рассчитать входящие в уравнения газовой динамики молярную массу и внутреннюю энергию смеси.

В соответствии с общепринятой практикой обобщенного моделирования кинетики детонационного сгорания газовых смесей, рассчитаем параметр индукции при переменных давлении и температуре по формуле:

$$Y = \int_0^{t_i} \frac{dt}{\tau_i} \quad , \tag{1}$$

где $\tau_i$ – период индукции при постоянных параметрах (Аррениусовская формула для расчета $\tau_i$ полагается известной). В начале периода индукции $Y = 0$, а в его конце ($t = t_i$) $Y = 1$.

Отметим, что величина $\beta$ влияет только на параметры волны внутри зоны индукции. Скорость волны и параметры потока в плоскости Чепмена-Жуге, а также протяженность зоны основного тепловыделения и профили потока внутри нее от величины $\beta$ не зависят. Таким образом, неточность в вычислении $\beta$ лишь

количественно повлияет на профиль параметров волны внутри индукционной зоны. Как правило, скорость химического превращения растет по мере истечения периода индукции. Поэтому можно использовать следующую формулу для вычисления $\beta$, которая удовлетворяет приведенным выше условиям:

$$\beta = 1 - Y. \tag{2}$$

Это соотношение позволяет рассчитать величину $\beta$ в любой момент времени.

После окончания периода индукции (в зоне основного тепловыделения детонационной волны) детальный химический состав смеси не вычисляется, а молярная масса газа рассчитывается с помощью одного обыкновенного дифференциального уравнения:

$$\frac{d\mu}{dt} = 4K_+ \frac{\rho^2}{\mu}\left(1 - \frac{\mu}{\mu_{\max}}\right)^2 - AT^{3/4}(1-\exp(-\theta/T))^{3/2}\rho\left(\frac{\mu}{\mu_{\min}} - 1\right)\exp(-E/RT). \tag{3}$$

Полная внутренняя энергия смеси вычисляется по формуле:

$$U(T,\mu) = U_{therm}(T,\mu) + U_{chem}(\mu), \tag{4}$$

$$U_{therm}(T,\mu) = \left[\frac{3}{4}\left(\frac{\mu}{\mu_a} + 1\right) + \frac{3}{2}\left(\frac{\mu}{\mu_a} - 1\right)\frac{\theta/T}{\exp(\theta/T)-1}\right]\frac{RT}{\mu}, \tag{5}$$

$$U_{chem}(\mu) = E\left(\frac{1}{\mu} - \frac{1}{\mu_{\min}}\right), \tag{6}$$

где $\rho$, $T$ и $\mu$ плотность, температура и средняя молярная масса смеси;

$R$ – универсальная газовая постоянная;

$\mu_a$ $\mu_{min}$ $\mu_{max}$ – молярные массы смеси в атомарном, предельно диссоциированном и преднльно рекомбинированном и состояниях;

$A$ и $K_+$ – константы скоростей диссоциации и рекомбинации обобщенных продуктов реакции;

$\theta$ – эффективная температура возбуждения колебательных степеней свободы молекул;

$E$ – средняя энергия диссоциации продуктов реакции;

$U$, $U_{therm}$ и $U_{chem}$ – полная удельная внутренняя энергия смеси, ее термодинамическая и химическая части.

Предлагаемая модель кинетики описывает и состояние химического равновесия, в котором $d\mu/dt = 0$. В этом случае молярная масса газа, показатель адиабаты, внутренняя энергия смеси и тепловой эффект химической реакции, как функции давления и температуры рассчитываются по явным алгебраическим формулам. Константы предложенной модели кинетики имеют четкий физический смысл.

Предложенная модель проста (она включает в себя явные алгебраические формулы и одно дифференциальное уравнение для описания зоны основного тепловыделения). Модель позволяет существенно сократить объем численных расчетов и упростить анализ полученных результатов по сравнению с моделями детальной химической кинетики, включающими в себя громоздкие системы жестких обыкновенных дифференциальных уравнений. В то же время предложенная модель обладает высокой точностью. Параметры волны Чепмена-Жуге (скорость, давление и температура), рассчитанные по предложенной модели, лишь на несколько процентов отличаются от соответствующих значений, рассчитанных с учетом детальной системы химического равновесия. Модель согласована со вторым началом термодинамики и удовлетворяет принципу Ле-Шателье, позволяя описывать сдвиг химического равновесия.


### *Благодарности*

Работа выполнена при финансовой поддержке РФФИ (код Проекта 18-58-53031 ГФЕН_а).


### БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Ю.А. Николаев, А.А. Васильев, В.Ю. Ульяницкий. Газовая детонация и ее применение в технике и технологиях (обзор). Физика горения и взрыва, 2003, т. 39, № 4, с. 22-54.

2. P.A. Fomin, A.V. Trotsyuk, A.A. Vasil'ev. Approximate model of chemical reaction kinetics for detonation processes in mixture of $CH_4$ with air. Combustion Science and Technology, 2014, Vol. 186, № 10-11, P. 1716-1735.

3. Hui-Ning Yang, Jen-How Chen, Home-Jo Chiu, Ting-Jia Kao, Hsiao-Yun Tsai, Jenq-Renn Chen. Confined vapor explosion in Kaohsiung City – A detailed analysis of the tragedy in the harbor city. Journal of Loss Prevention in the Process Industries, 2016, V. 41, № 5, P. 107-120.

УДК 006: 621. 317.744
DOI: 10.33764/2618-981X-2019-9-77-86

# КОАКСИАЛЬНОЕ КОНТАКТНОЕ УСТРОЙСТВО И СПОСОБ ЕГО КАЛИБРОВКИ

***Наталья Викторовна Заржецкая***
Сибирский государственный университет геосистем и технологий, 630136, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры специальных устройств, инноватики и метрологии, тел. (913)456-07-97, e-mail: zarjetskaya@yandex.ru

***Владимир Анатольевич Литовченко***
Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, начальник инструкторской группы кафедры разведки (и воздушно-десантной подготовки), тел. (383)332-50-45, e-mail: litovchienko.vladimir@mail.ru; Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, аспирант, тел. (923)100-89-86

Предложено коаксиальное контактное устройство для подключения к анализатору СВЧ-цепей как коаксиальных мер при калибровке анализатора, так и исследуемых полосковых узлов при измерении их S-параметров. Кроме того, предложен способ калибровки этого устройства одним или двумя расчетными полосковыми калибраторами, обеспечивающий перенос результатов калибровки анализатора коаксиальными мерами на измерение S-параметров полосковых узлов.

**Ключевые слова:** коаксиальное контактное устройство, калибровка, измерение S-параметров.

# COAXIAL CONTACT DEVICE AND METHOD OF CALIBRATION

***Natalya V. Zarzhetskaya***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Special-Purpose Devices, Innovatics and Metrology, phone: (913)456-07-97, e-mail: zarjetskaya@yandex.ru

***Vladimir A. Litovchenko***
Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Head of Instructor Group, Department of Educational Intelligence (and Airborne Training), phone: (383)332-50-45, e-mail: litovchienko.vladimir@mail.ru; Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D. Student, phone: (923)100-89-86

A coaxial contact device for connection to the microwave transition analyzer is proposed as coaxial measures for calibrating the analyzer, and the investigated strip line junctions for measuring their S-parameters. In addition, a method for calibrating this device with one or two calculated coaxial-to-stripline calibrators, providing the transfer of the results of calibration of the analyzer by coaxial measures to the measurement of S-parameters of the strip line junctions is presented.

**Key words:** coaxial contact device, calibration, measurement of S-parameters of strip line junctions.

## *Введение*

Для калибровки анализаторов СВЧ-цепей (АЦ) [1] используют наборы однотипных стандартизированных мер отражения и проходных мер, например, коаксиальные или волноводные.

Исследуемые узлы могут иметь большое разнообразие типов входных трактов и чаще всего полосковых, для которых нет ни одного набора стандартизированных мер. Это приводит к необходимости разработки контактных устройств (КУ) [2-8] для подключения таких узлов к АЦ и способов калибровки КУ [2, 4, 8-10], обеспечивающих перенос результатов калибровки АЦ стандартизированными мерами на измерение *S*-параметров полосковых узлов.

В работах [2, 3] предложены конструкции и способы калибровки полосковых контактных устройств (ПКУ). Одним из существенных недостатков ПКУ является то, что они не обеспечивают подключение к АЦ стандартизированных мер при калибровке АЦ, что требует демонтажа ПКУ. К другим недостаткам ПКУ относятся плохая повторяемость подключения к ним расчетных полосковых калибраторов при калибровке ПКУ и исследуемых полосковых узлов при измерении их *S*-параметров, а также значительный собственный коэффициент стоячей волны (КСВ) и потери.

## *Методы и материалы*

В статье предложено коаксиальное контактное устройство (ККУ) [4-7] для подключения к АЦ как коаксиальных мер при калибровке АЦ, так и исследуемых полосковых узлов при измерении их *S*-параметров. Кроме того, предложен способ калибровки ККУ [4, 9] одним или двумя расчетными полосковыми калибраторами, обеспечивающий перенос результатов калибровки АЦ коаксиальными мерами на измерение *S*-параметров полосковых узлов.

**Конструкция.** Предлагаемое ККУ показано на рис. 1. ККУ содержит основание 1, на котором установлены коаксиальные переходы (КП) 2 с возможностью их перемещения вдоль центральной оси. Каждый из КП 2 снабжен контактной головкой 3, которая введена в его осевое отверстие с возможностью ее осевого перемещения и закрепления фиксаторами 4 в рабочем положении, как показано на рис. 1. Между КП 2 установлен съемный пьедестал 5, на котором закреплен исследуемый полосковый узел 6, подключение которого к КП 2 осуществляется подпружиненными цангами 7 контактных головок 3. Полное введение контактных головок 3 в осевые отверстия КП 2 приводит к перекрытию «тромбонов» 8, образованных КП 2 и контактными головками 3, что исключает возможность излучения СВЧ-энергии при подключении узла 6. Возможность замены контактных головок 3 и пьедестала 5 обеспечивает подключение к ККУ узлов в виде планарных структур с различными базовыми длинами $l$, соответствующими расстоянию между плоскостями 1-1$'$ и 2-2$'$ подключения этих узлов. Так, например, на рис. 1, *а* показано подключение полевого транзистора

с барьером Шоттки (ПТБШ) 6, а на рис. 1, *б* – отрезка микрополосковой линии (МПЛ) 9, в которую включен кристалл 10 безкорпусного транзистора. Выбор требуемой базовой длины *l* осуществляется путем замены пьедестала 5. Возможность осевого перемещения контактных головок 3 при подключении узла 6 исключает необходимость перемещения КП 2 а, следовательно, погрешность измерений, вносимую деформациями кольцевого измерительного канала АЦ. Этому также способствует пьедестал аналогичный пьедесталу 5, снабженный проходной коаксиальной мерой для калибровки АЦ «на проход» с длиной *l* меры равной базовой длине узла 6. При малой длине *l* калибровку АЦ «на проход» осуществляют при непосредственном соединении плоскостей 1-1' и 2-2' входов КП 2. При этом соединение центральных проводников контактных головок 3 осуществляется подпружиненной цангой 7 с большим усилием пружины, а внешних проводников – с помощью одной из подвижных резьбовых втулок 11.

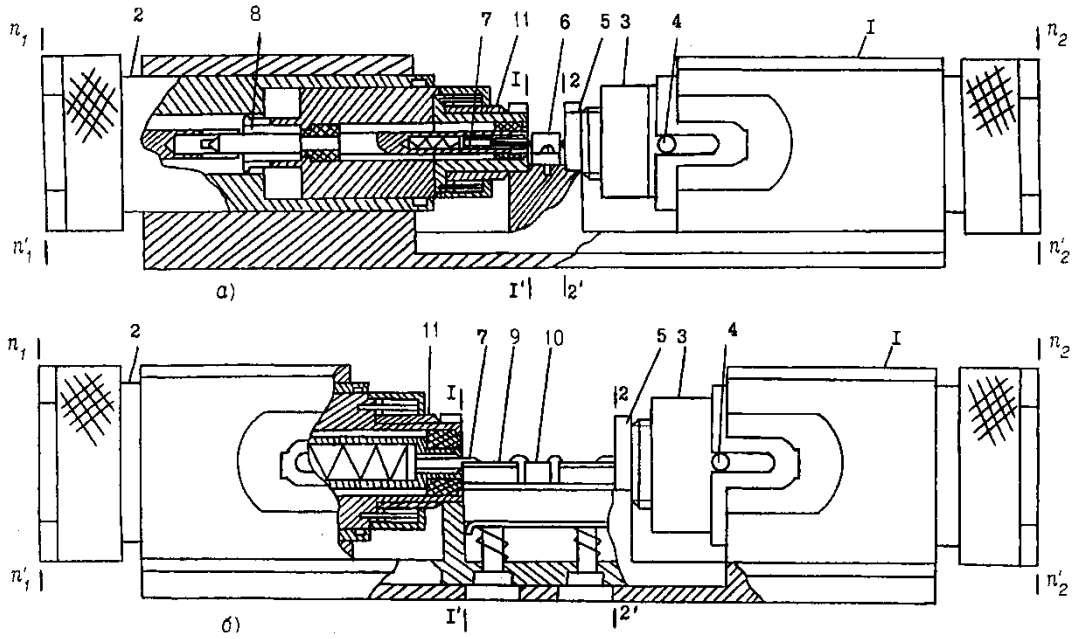



Рис. 1. Коаксиальное контактное устройство

Технические характеристики ККУ:
Диапазон рабочих частот: 0,1-18 ГГц.
Потери на КП: не более 0,5 дБ.
КСВ: не более 1,15.
Тип подключаемых узлов:
устройства с коаксиальными разъемами 3,5/1,5 мм;
транзисторы в корпусах КТ-21, КТ-22, КТ-47, 048-03 и 048-04;
полосковые структуры с базовой длиной 5, 12, 24 и 48 мм.
Погрешность, вносимая ККУ из-за неповторяемости подключения
Модуля: не более 1%, фазы: не более 1 град.
Габариты: 220х45х45 мм.

**Способ калибровки.** Возможность подключения коаксиальных мер 12 к АЦ посредством КП 2 позволяет осуществить калибровку АЦ относительно плоскостей $i$-$i'$ входов КП 2 (рис. 2).

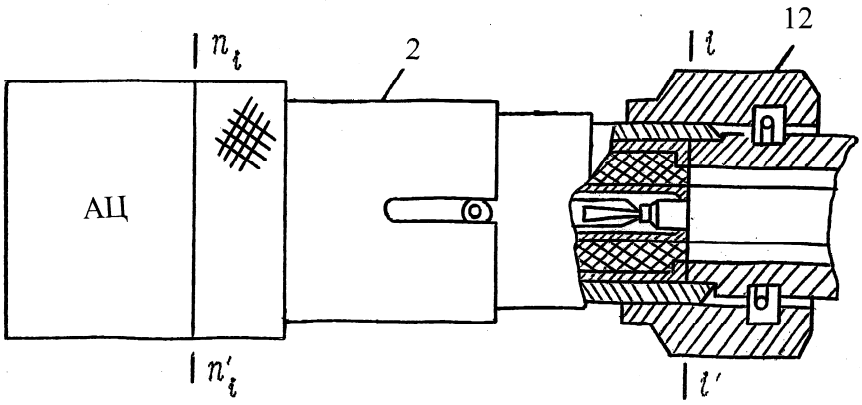



Рис. 2. Калибровка АЦ

Для переноса результатов калибровки АЦ коаксиальными мерами на измерение $S$-параметров полосковых узлов необходима калибровка КП 2 расчетными полосковыми калибраторами, например, отрезками МПЛ с волновым сопротивлением $Z_0$, нагруженными на согласованные нагрузки $Z_H = Z_0$, или проходными микрополосковыми калибраторами в виде двух отрезков МПЛ с волновым сопротивлением $Z_0$, имеющих различную длину $l_k$ (рис. 3), где $k$ = 1, 2 – индекс проходного микрополоскового калибратора.

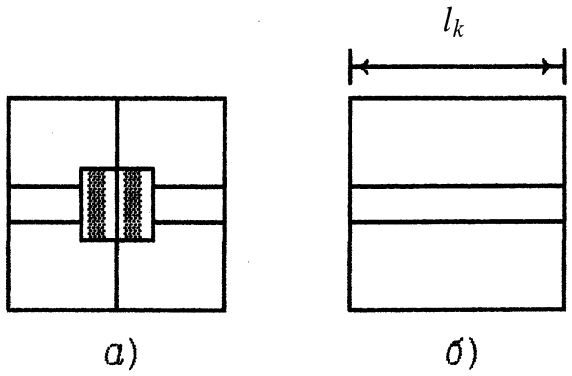



Рис. 3. Согласованный (*а*) и проходной (*б*)
микрополосковые калибраторы

Конструктивное различие КП 2 (рис. 2), и согласованного микрополоскового калибратора (рис. 3, *а*), приводит к тому, что комплексные коэффициенты отражения (ККО) $\Gamma_i^0$ этого калибратора в плоскостях $i$ - $i'$ подключения его

к входам КП 2 не равны нулю $\Gamma_i^0 \neq 0$ (рис. 4, *а*). Это требует введения в рассмотрение вспомогательных плоскостей $B_i - B_i^{'}$ соответствующих плоскостям входов согласованного микрополоскового калибратора, в которых его ККО $\Gamma_i^0 = 0$. Введение этих плоскостей требует включения между ними и плоскостями $i$-$i^{'}$ 4-х-полюсника переноса с неизвестными $R_i$-параметрами рассеяния (рис. 4), где $S_{ijk} = C_k \exp(\varphi_{ijk})$ - $S_k$ – параметры $k$-го проходного микрополоскового калибратора; $C_k$ и $\varphi_{ijk} = -j\beta l_k$ – их модуль и фаза; $\beta = 2\pi/\lambda$ и $\lambda = c/\sqrt{\varepsilon_э} f$ – фазовая постоянная и длина волны в отрезках МПЛ согласованного и проходных микрополосковых калибраторов; $\varepsilon_э$ – эффективная диэлектрическая проницаемость МПЛ.

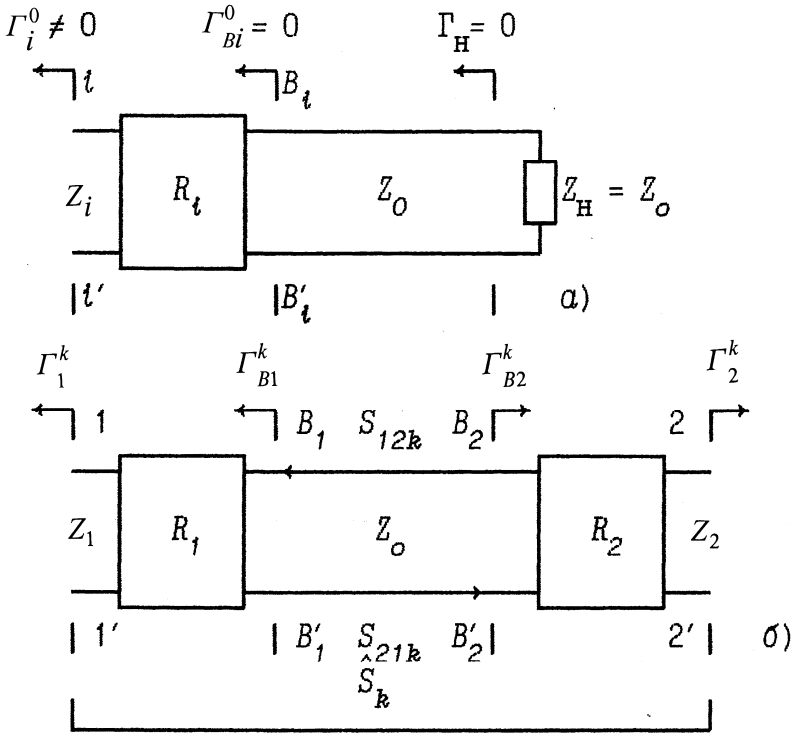



Рис. 4. Эквивалентная схема замещения ККУ при включении в него согласованного (*а*) и проходного (*б*) микрополосковых калибраторов

Таким образом, задача калибровки ККУ решается посредством измерения ККО $\Gamma_i^0$ или $\hat{S}_k$-параметров в плоскостях $i$ - $i^{'}$ входов КП 2 при подключении к ним согласованного микрополоскового калибратора или поочередного под-

ключения двух проходных микрополосковых калибраторов, имеющих длину $l_k$, с последующим определением $R_i$-параметров 4-х-полосников переноса. По измеренным ККО $\Gamma_i^0$ или $\hat{S}_k$-параметрам $R_{11i}$-параметры можно определить как в [10]:

$$R_{11i} = \Gamma_i^0,$$

$$R_{11i} = (\hat{S}_{iij}\hat{S}_{iji}e^{j\beta l_j} - \hat{S}_{iii}\hat{S}_{ijj}e^{j\beta l_i})/(\hat{S}_{iji}e^{j\beta l_j} - \hat{S}_{ijj}e^{j\beta l_i}), \qquad (1)$$

$$i, j=1,2,\ i \neq j.$$

Для определения недостающих $R_{21i}$ и $R_{22i}$-параметров 4-х -полюсники переноса (рис. 4), были представлены параллельной проводимостью $Y_{Ri}$. Такое представление сделано в предположении физического совпадения плоскостей $i$ - $i'$ и $B_i - B_i'$.

Падающие и отраженные волны $U_{1i}^{\pm}$ и $U_{2i}^{\pm}$ связаны в плоскостях $i$ - $i'$ и $B_i - B_i'$ уравнениями:

$$\left.\begin{aligned} U_{1i}^{-} &= r_{11i}U_{1i}^{+} + r_{12i}U_{2i}^{+} \\ U_{2i}^{-} &= r_{21i}U_{1i}^{+} + r_{22i}U_{2i}^{+} \end{aligned}\right\}, \qquad (2)$$

где $r_i$ – ненормированные параметры рассеяния 4-х - полюсников переноса.

Из системы уравнений (2) при $U_{1i} = U_{2i}$, где $U_{1i} = U_{1i}^{+} + U_{1i}^{-}$ и $U_{2i} = U_{2i}^{+} + U_{2i}^{-}$, получим

$$U_{1i}^{+}[(1 - r_{21i}) + r_{11i}] = U_{2i}^{+}[(1 - r_{12i}) + r_{22i}]. \qquad (3)$$

Уравнение (3) имеет решение:

$$r_{12i} = 1 + r_{11i}, r_{21i} = 1 + r_{22i}, \qquad (4)$$

которое после его нормировки с учетом того, что $r_{11i} = R_{11i}$ и $r_{22i} = R_{22i}$ можно представить в виде:

$$R_{12i} = (1 + R_{22i})\sqrt{Z_0 / Z_i},\ R_{21i} = (1 + R_{11i})\sqrt{Z_i / Z_0}, \qquad (5)$$

где $Z_i$ – волновое сопротивление КП 2, равное волновому сопротивлению коаксиальных мер, используемых при калибровке АЦ.

Применяя к (5) условие взаимности $R_{12i} = R_{21i}$, определим недостающие $R_{12i}$, $R_{21i}$ и $R_{22i}$-параметры:

$$R_{12i} = R_{21i} = (1 + R_{11i})\sqrt{Z_i / Z_0},\ R_{22i} = (1 + R_{11i})Z_i / Z_0 - 1. \quad (6)$$

Калибровку ККУ при измерении *S*-параметров предпочтительнее выполнять двумя проходными микрополосковыми калибраторами, а при измерении *Г*-параметров – согласованными (рис. 3). Причем, нормировка (6) $R_i$-параметров может быть осуществлена относительно произвольного волнового сопротивления $Z_0$ согласованного микрополоскового калибратора и двух проходных микрополосковых калибраторов, выбранных для калибровки ККУ.

Таким образом, предложен способ калибровки ККУ, описывающийся математической моделью (1) и (6).

**Определение S-параметров.** В общем случае ККУ с включенным в него исследуемым полосковым узлом представляет собой каскадное соединение 4-х-полюсников с $\hat{S} = f(R_1, S, R_2)$-параметрами.

*S*-параметры узла можно определить из выражений [4, 11–19]:

$$S_{11} = [R_{112}(R_{111}\hat{S}_{22} - \hat{\Delta}_S) + (\hat{S}_{11} - R_{111})\Delta_{R2}] / \Delta_S,$$

$$S_{12} = -R_{211}R_{212}\hat{S}_{12} / \Delta_S, \quad (7)$$

$$S_{21} = -R_{121}R_{122}\hat{S}_{21} / \Delta_S,$$

$$S_{22} = [R_{221}(R_{222}\hat{S}_{11} - \hat{\Delta}_S) + (\hat{S}_{22} - R_{222})\Delta_{R1}] / \Delta_S,$$

где

$$\hat{\Delta}_S = \hat{S}_{11}\hat{S}_{22} - \hat{S}_{12}\hat{S}_{21};$$

$$\begin{aligned} \Delta_{R1} &= R_{111}R_{221} - R_{121}R_{211}; \\ \Delta_{R2} &= R_{112}R_{222} - R_{122}R_{212}; \end{aligned} \quad (8)$$

$$\Delta_S = R_{112}(\hat{S}_{22}\Delta_{R1} - R_{221}\hat{\Delta}_S) + (R_{221}\hat{S}_{11} - \Delta_{R1})\Delta_{R2};$$

$\hat{S}_{ii}$ и $\hat{S}_{ij} - \hat{S}$-параметры узла, измеренные в плоскостях $i - i'$ его подключения к ККУ.

Выражения (7) обеспечивают перенос результатов калибровки АЦ коаксиальными мерами на измерение *S*-параметров полосковых узлов. При измерении *S*-параметров коаксиальных узлов $S = \hat{S}$ .

## *Заключение*

Предложенное ККУ [20–27] имеет более широкие функциональные возможности в сравнении с ПКУ. ККУ обеспечивает подключение к АЦ как коаксиальных мер, так и исследуемых полосковых узлов с разнообразными типами входных полосковых трактов. Кроме того, ККУ обеспечивает высокую повторяемость подключения к нему коаксиальных мер и исследуемых полосковых узлов, имеет малый собственный КСВ и потери. Для калибровки ККУ используется минимальный набор легко рассчитываемых микрополосковых калибраторов, что с учетом высокой повторяемости их подключения уменьшает погрешность измерения вносимую ККУ в сравнении с ПКУ в 2–3 раза.

## *Благодарности*

Авторы выражают благодарность за помощь и поддержку своему научному руководителю, Савелькаеву Сергею Викторовичу, д.т.н., профессору СГУГиТ.

### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Савелькаев, С.В. Теоретические основы построения адаптивных цифровых анализаторов СВЧ-цепей // Электрон. техника. Сер. Электроника СВЧ. - 1991. - Вып. 9. - С. 34 - 39.

2. А.с. 1478156 СССР, G 01 R 27/28. Держатель транзисторов в устройствах для измерения электрических параметров/В.П. Петров, С.В. Савелькаев. - Опубл. Бюл.//Открытия. Изобретения. - 1989. - №17.

3. А.с. 1682942 СССР, G 01 R 27/28. Держатель транзисторов в устройствах для измерения электрических параметров/В.П. Петров, С.В. Савелькаев, А.В. Борисов. - Опубл. Бюл. // Открытия. Изобретения. - 1991. - №37.

4. Савелькаев, С.В. Коаксиальное контактное устройство / С.В. Савелькаев // Электрон. техника. Сер. Электроника СВЧ. - 1991.- Вып.6. - С. 30 - 33.

5. А.с. 1436152 СССР, H 01 P 5/08. Контактное устройство / С.В. Савелькаев. - Опубл. Бюл. // Открытия. Изобретения. – 1988. - №41.

6. А.с. 1608762 СССР, H 01 P 5/08. Контактное устройство / С.В. Савелькаев. - Опубл. Бюл.//Открытия. Изобретения. - 1990. - №43.

7. А.с. 1584001 СССР, H 01 P 5/08. Контактное устройство / С.В. Савелькаев, А.П. Герасименко. - Опубл. Бюл.//Открытия. Изобретения. - 1990. - №29.

8. А.с. 11578667 СССР, H 01 P 5/08. Контактное устройство и калибровочная согласованная нагрузка/С.В. Савелькаев, А.П. Герасименко. - Опубл. в Бюл. // Открытия. Изобретения. – 1990. - №26.

9. А.с. 1774286 СССР, G 01 R 27/28. Способ калибровки коаксиального устройства/ С.В. Савелькаев. - Опубл. Бюл. // Открытия. Изобретения, - 1992. - №41.

10. Гупта К., Гардж Р., Чадха Р. Машинное проектирование СВЧ-устройств. – М.: Радио и связь, 1987 – 432 с.

11. Теоретические основы построения имитатора-анализатора активных СВЧ-цепей / С. В. Савелькаев, С. В. Ромасько, В. А. Литовченко, Н. В. Заржецкая // Вестник СГУГиТ. – 2016. – Вып. 1 (33). – С. 175–188.

12. Теоретические основы построения имитатора-анализатора активных СВЧ-цепей / С. В. Савелькаев, С. В. Ромасько, В. А. Литовченко, Н. В. Заржецкая // Успехи современной радиотехники. – 2017. – № 2. – С. 50–61.

13. Теоретические основы построения имитатора-анализатора усилителей и автогенераторов СВЧ / С. В. Савелькаев, С. В. Ромасько, В. А. Литовченко, Н. В. Заржецкая // Известия высших заведений России. Радиоэлектроника. – 2017. – Вып. 1. – С. 63–74.

14. Савелькаев С. В., Заржецкая Н. В. Расчет и проектирование автогенераторов СВЧ в пространстве S-параметров // Известия высших заведений России. Радиоэлектроника. – 2016. – Вып. 1. – С. 41–53.

15. Полупроводниковые входные устройства СВЧ / Под редакцией В. С. Эткина. – М. : Сов. Радио, 1975, Т. 1. – 344 с.

16. Савелькаев С. В., Ромасько С. В., Литовченко В. А. Математическая модель имитатора-анализатора усилителей и автогенераторов СВЧ // Интерэкспо ГЕО-Сибирь-2017. XIII Междунар. науч. конгр. : Национ. науч. конф. «Наука. Оборона. Безопасность-2017» : сб. материалов (Новосибирск, 17–21 апреля 2017 г.). – Новосибирск : СГУГиТ, 2017. – С. 131–137.

17. Савелькаев С. В., Айрапетян В. С., Литовченко В. А. Методика расчета автогенератора СВЧ в пространстве S-параметров // Интерэкспо ГЕО-Сибирь-2014. X Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2014» : сб. материалов в 2 т. (Новосибирск, 8–18 апреля 2014 г.). – Новосибирск : СГГА, 2014. Т. 2. – С. 164–171.

18. Литовченко В. А. Методы анализа устойчивости активных СВЧ-цепей и измерения их S-параметров // Вестник СГУГиТ. – 2015. – Вып. 1 (29). – С. 90–100.

19. Савелькаев С. В., Айрапетян В.С., Литовченко В. А. Трехсекционная дрейфово-диффузионная математическая модель полевого транзистора с барьером шоттки // Вестник НГУ. Серия: Физика твердого тела, полупроводников наноструктур. – 2015. – Том 10, № 1. – С. 57–62.

20. Савелькаев С. В., Литовченко В. А. Способ калибровки полоскового контактного устройства // Интерэкспо ГЕО-Сибирь-2016. XII Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2016» : сб. материалов в 2 т. (Новосибирск, 18–22 апреля 2016 г.). – Новосибирск : СГУГиТ, 2016. Т. 3. – С. 37–41.

21. Савелькаев С. В., Литовченко В. А. Методика расчета автогенератора СВЧ, в пространстве S-параметров // Электромагнитные волны и электронные системы. – 2016. – № 8. – С. 36–46.

22. Метод анализа устойчивости активных СВЧ-цепей / С. В. Савелькаев, С. В. Ромасько, В. А. Литовченко, Н. В. Заржецкая // Интерэкспо ГЕО-Сибирь-2016. XII Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2016» : сб. материалов в 2 т. (Новосибирск, 18–22 апреля 2016 г.). – Новосибирск : СГУГиТ, 2016. Т. 5. – С. 224–228.

23. Анализ высокоточных методов измерения параметров отражения в коаксиальных трактах / С. В. Владимирова, Ю. А. Пальчун [и др.] // Вестник ТГТУ. – 2012. – Т. 18, № 4. – С. 856–862.

24. Владимирова С. В., Пальчун Ю. А., Колпаков А. В. Использование интерполирующих и экстраполирующих функций для определения межповерочного интервала коаксиальных мер // ГЕО-Сибирь-2010. VI Междунар. науч. конгр.: сб. материалов в 6 т. (Новосибирск, 19–29 апреля 2010 г.). – Новосибирск : СГГА, 2010. Т. 5, ч. 2. – С. 127–129.

25. Владимирова С. В., Пальчун Ю. А. Алгоритмические методы определения функции поправки по модулю при измерении параметров отражения // ГЕО-Сибирь-2011. VII Междунар. науч. конгр. : сб. материалов в 6 т. (Новосибирск, 19–29 апреля 2011 г.). – Новосибирск : СГГА, 2011. Т. 5, ч. 2. – С. 261–263.

26. Ромасько С. В. Методика определения коэффициентов интерполяции и экстраполяции СВЧ мер ослабления по модулю коэффициента отражения // Интерэкспо ГЕО-Сибирь-2015. XI Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2015» : сб. материалов в 3 т. (Новосибирск, 13–25 апреля 2015 г.). – Новосибирск : СГУГиТ, 2015. Т. 2. – С. 127–129.

27. Савелькаев С. В., Литовченко В. А. Вариационная методика оценки суммарной погрешности измерения имитаторв-анализаторов усилителей и автогенераторов СВЧ // Интерэкспо ГЕО-Сибирь. XIV Междунар. науч. конгр. : Междунар. науч. конф. «Наука. Оборона. Безопасность-2018» : сб. материалов (Новосибирск, 23–27 апреля 2018 г.). – Новосибирск : СГУГиТ, 2018. – С. 3–12.

УДК 621.396.67
DOI: 10.33764/2618-981X-2019-9-87-97

# ПРЕИМУЩЕСТВА ШИРОКОПОЛОСНОГО (ИК-ТГЦ) ЛОЦИРОВАНИЯ ОБЪЕКТОВ ПРИ НАЛИЧИИ ПОМЕХ

***Александр Григорьевич Черевко***
Сибирский государственный университет телекоммуникаций и информатики, 630102, Россия, г. Новосибирск, ул. Кирова, 86, кандидат физико-математических наук, зав. кафедрой физики, тел. (913)980-60-71, e-mail: persp14@mail.ru

***Валерик Сергеевич Айрапетян***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, зав. кафедрой специальных устройств, инноватики и метрологии, тел. (913)462-10-75, e-mail: V.hayr10004@mail.ru

***Валерий Григорьевич Эдвабник***
АО «Научно-исследовательский институт электронных приборов», 630005, Россия, г. Новосибирск, ул. Писарева, 53, доктор экономических наук, заместитель генерального директора по развитию АО «НИИЭП», тел. (383)216-05-52

Рассматриваются преимущества широкодиапазонного (ИК-ТГц) опознавания объектов в условиях дымовых, пылевых завес и тумана. Показано, что лоцирование объектов в диапазоне ИК-ТГц обеспечит опознавание объектов в указанных условиях. Приведены результаты локации объектов в ТГц диапазоне, дающие информацию об ЭПР объекта и результаты локации в ИК диапазоне. Сравнение затухания сигнала ИК и ТГц диапазона в условиях дымовых, пылевых завес и тумана указывают на необходимость объединения этих диапазонов для решения задач лоцирования объектов в условиях реальных помех, возникающих в боевых, антитеррористических операциях и при чрезвычайных ситуациях.

**Ключевые слова:** терагерцы; ИК, ТГц излучение; пылевые, дымовые завесы, лоцирование; коэффициент пропускания.

# BROADBAND IDENTIFICATION OF OBJECTS-ADVANTAGES IN DIFFICULT INTERFERENCE

***Alexander G. Cherevko***
Siberian State University of Telecommunications and Information Sciences, 86, Kirova St., Novosibirsk, 630102, Russia, Ph. D., Head of Physics Department, phone: (913)980-60-71, e-mail: persp14@mail.ru

***Valerik S. Ayrapetyan***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Head of Special Devices, Innovations and Metrology Department, phone: (913)462-10-75, e-mail: V.hayr1004@mail.ru

***Valery G. Edvabnik***
Scientific Research Institute of Electronic Devices, 53, Pisareva St., Novosibirsk, 630005, Russia, D. Sc., Deputy Director General for Development, phone: (383)216-05-52

The advantages of wide-range (IR THz) identification of objects in smoke, dust curtains and fog are considered. It is shown that the identification of objects in these conditions is provided by using extended (IR THz) range. The results of the object location in the THz range, giving information about the ESR of the object, and the results of the location in the IR range are presented. Comparison of the attenuation of the IR and THz signal in the conditions of smoke, dust curtains and fog indicate the need to combine these ranges to solve the problems of locating objects in conditions of real interference arising in combat, antiterrorist operations and in emergency.

**Key words:** IR, THz radiation, dust, smoke curtains, locating; transmittance, absorptance.

## *Введение*

Современное высокоточное оружие широко использует системы наведения инфракрасного диапазона в окнах прозрачности атмосферы ~ (1–10) мкм, что обеспечивает необходимую точность лоцирования объекта, который не скрыт пылевыми, дымовыми завесами или туманом. В присутствии этих мешающих факторов поглощение ИК излучения заметно, даже на порядки, возрастает, и система наведения может сработать нештатно. Такой результат объясняется релеевским рассеиванием ИК излучения, при котором сечение рассеяния растет как $(1/\lambda^4)$. Современные конфликты сопровождаются значительным задымлением и часто происходят в регионах, где возникают песчаные бури. Антитеррористические операции могут сопровождаться дымовыми завесами, такие же помехи возникают и при чрезвычайных ситуациях. Системы наведения должны работать в условиях тумана, где также существенно релеевское рассеяние излучения. Кроме того, дымовые и пылевые завесы устанавливают объекты для экстренной маскировки. Таким образом, актуальной задачей является повышение эффективности систем наведения, работающих в условиях пылевых, дымовых завес и тумана. Задача может быть решена путем использования широкополосной системы наведения, использующей ИК и ТГц диапазон. Такой подход решает проблему релеевского рассеивания, обеспечивая необходимую точность систем наведения.

## *Методы и материалы*

Терагерцовый диапазон частот электромагнитного спектра (ТГц-диапазон) лежит между областью миллиметровых длин волн и инфракрасным диапазоном. Граничные частоты ТГц-диапазона в настоящее время точно не определены и в разных источниках определяются по-разному. В наиболее широкой интерпретации ТГц-диапазон занимает область частот от 100 ГГц до 10 ТГц (диапазон длин волн от 3 мм до 30 мкм). Учитывая эту интерпретацию, логику ГОСТ 24375-80 и рекомендации Международного союза электросвязи в настоящей работе к ТГц-диапазону отнесем диапазон частот 0,3 – 10 ТГц (30-1000 мкм). Таким образом, ТГц-диапазон является областью сближения электроники и фотоники, существенно отличающихся как теоретической базой, так и техникой генерацей, осуществления приема и обработки электромагнитных волн. В основе традиционной электроники лежит классическая теория электромагнетизма

и теория переноса, описывающая электрон-дырочное взаимодействие и возникающее в результате излучение, в то время как в основе фотоники лежат квантомеханические принципы взаимодействия излучения и материи.

Статистический анализ патентной активности, проведенный авторами с использованием открытых источников, в частности [1, 2], показал, что наблюдается линейный рост числа патентов, в этой области, начиная с 2000 года (рис. 1).

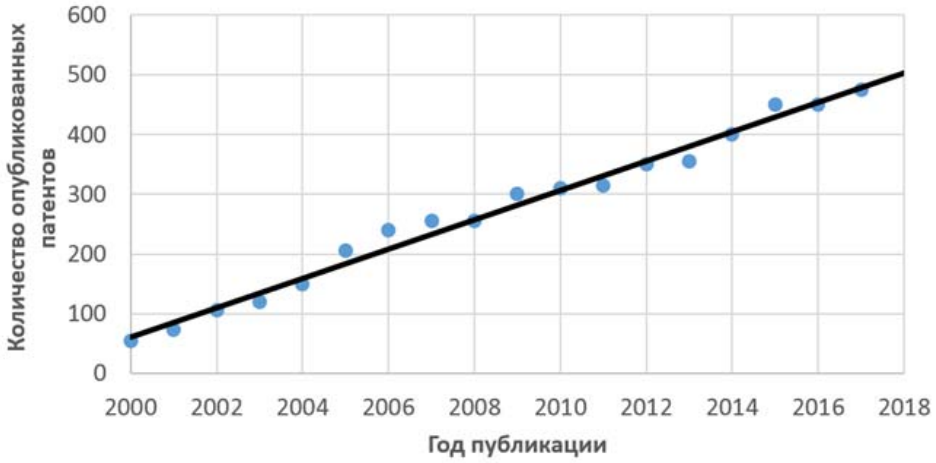



Рис. 1. Мировая тенденция развития ТГц локации
(по материалам патентных исследований)

Статистический анализ результатов поиска по странам приоритета показал, что наибольшее число патентов в исследуемой области выдано в странах НАТО, а также США, Китае, Японии (рис. 2). Достаточно большое количество подано в качестве международных заявок. Из рисунка видно, что число Российских патентов в этой области на порядок меньше, чем патентов США, что указывает на актуальность проблемы, поставленной в настоящем исследовании.

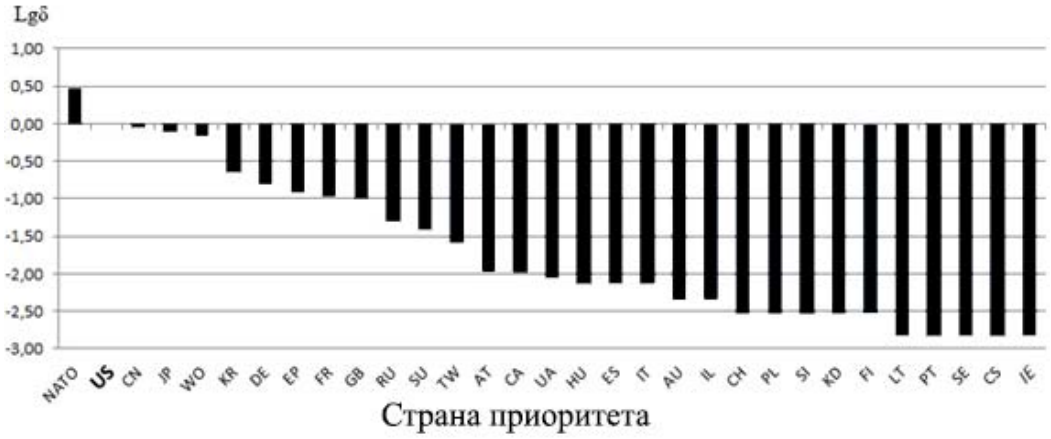



Рис. 2. Относительное число зарегистрированных патентов по ТГц локации
($\delta = N_K/N_{US}$, где$N_{US}$ − число патентов, зарегистрированных в США)

Из рис. 3 видно, что максимум излучения абсолютно черного тела (АЧТ) с температурой Т = 20 – 50 К находится в ТГц диапазоне. Таким образом, холодные объекты в стратосфере и космосе всегда излучают в ТГц диапазоне, при этом, как следует из рис.3 в полосе поглощения шириной в 1 мкм на детектор площадью в 1 см$^2$ будет падать излучение мощностью от $4 \cdot 10^{-9}$ до $4 \cdot 10^{-7}$ Вт и, при соответствующей пороговой чувствительности приемника, которая в настоящее время достигнута, это излучение будет зарегистрировано. В результате, можно утверждать, что ТГц локация имеет фундаментальную базу, по крайней мере, для пассивной, наименее уязвимой ее части. Высказанное утверждение подтверждается тем фактом, что для изучения космических объектов созданы радиотелескопы, работающие именно в ТГц диапазоне.

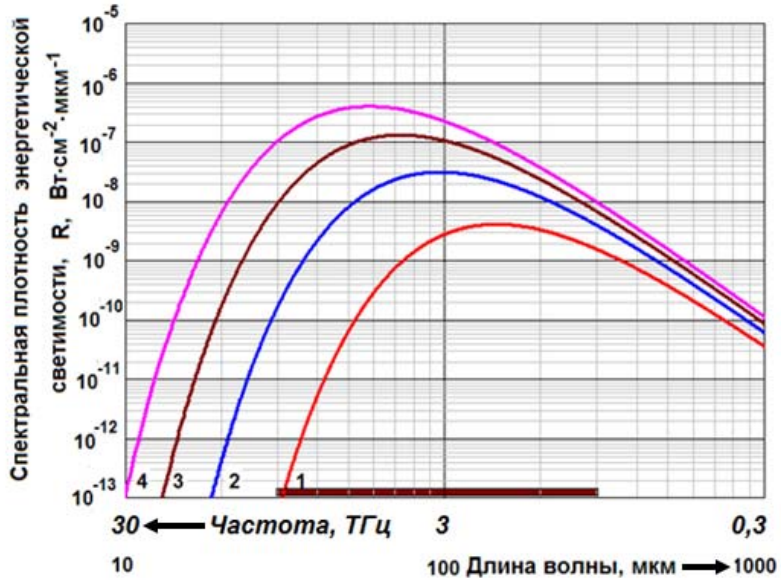



Рис.3. Частотная зависимость спектральной плотности энергетической светимости АЧТ при различных температурах АЧТ. 1 – Т=20 К; 2 – 30 К; 3 – 40 К; 4 – 50 К. Залитый прямоугольник – область дальнего ТГц диапазона

## *Результаты*

*Анализ окон пропускания в ТГц диапазоне.*

К сожалению, следует отметить малое количество экспериментальных данных о ТГц рассеянии в тумане, дожде, аэрозольных смесях и т.д. пробел связан с отсутствием достаточного количества источников монохроматического ТГц излучения. В настоящее время существует один тип надежного мощного монохроматического ТГц излучения – это лазеры на свободных электронах (ЛСЭ). Таких лазеров в мире считанное количество. При этом единственный в России и самый мощный в мире источник ТГц излучения – это Новосибирский ЛСЭ (НЛСЭ), характеристики которого представлены в табл. 1.

*Таблица 1*

Характеристики Новосибирского ЛСЭ

| № п/п | Параметр | Величина |
|---|---|---|
| 1 | Средняя мощность | 100−300 Вт |
| 2 | Пиковая мощность | 300−900 кВт |
| 3 | Частота повторения импульсов | 5,6 МГц |
| 4 | Длительность импульса | (60…100) пс |
| 5 | Диапазон перестройки длин волн, **λ,** (частот) | (0.03–0.24) мм<br>(1.3–10.0) ТГц |
| 6 | Относительная ширина спектра | 0,2–0,5 % |
| 7 | Исходная поляризация<br>(степень поляризации излучения) | Линейная<br>(> 99,6 %) |
| 8 | Поперечная когерентность | Полная |
| 9 | Временная когерентность | (40 … 100) пс |
| 10 | Диаметр гауссова пучка на выходе метрологической станции | 50−100 мм |
| 11 | Расходимость излучения | Дифракционная |

Настоящая работа, как мы надеемся, при своем развитии позволит в дальнейшем поставить необходимые эксперименты с НЛСЭ и получить надежные данные по поглощению ТГц излучения. Как следует из характеристик НЛСЭ (табл. 1) важными преимуществами этого прибора является большая мощность в непрерывном режиме, возможность плавной регулировки длины волны его излучения и стабильная частота следования импульсов, что позволяет применить синхронное детектирование и повысить чувствительность экспериментальной установки.

Среди расчетных работ представляет интерес статья [3], где допускается существование окон пропускания в ТГц диапазоне, в частности, предполагаемое окно при 7,2 ТГц имеет коэффициент пропускания сравнимый с сантиметровым диапазоном, т.е. пригодно для создания дальнодействующего ТГц локатора (рис.4). Таким образом, вопрос об окнах пропускания ТГц диапазона остается открытым и требует экспериментальных исследований, поскольку теоретические модели недостаточно точны. Такой эксперимент возможно поставить на основе НЛСЭ.

*Экспериментальные результаты, подтверждающие возможность ТГц локации.*

Авторами разработана экспериментальная установка [4] и проведены измерения ЭПР сложных объектов (рис.5) с использованием НЛСЭ в качестве источника (длина волны 130 мкм). Как видно из рисунка разработка ТГц канала системы наведения имеет практические перспективы.

На рис. 5 приведен экспериментальный результат, когда модель облучается со стороны крыльев. При этом наблюдается минимальное рассеяние (минимальная ЭПР). Здесь существенный вклад могут давать кили хвостового оперения модели.

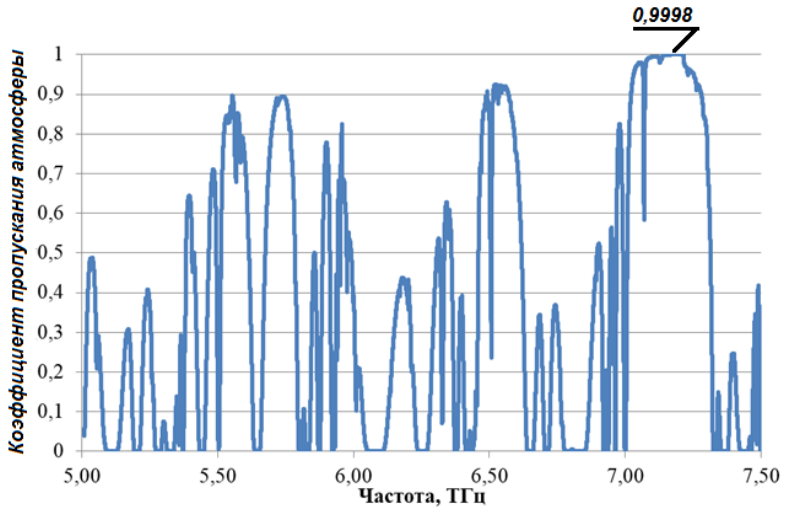



Рис. 4. Коэффициент пропускания атмосферы на уровне моря,
средняя широта, лето, стандартная американская модель 1976 года.
Расчет Института оптики атмосферы им. В.Е.Зуева СО РАН (ИОА СО РАН) [3]

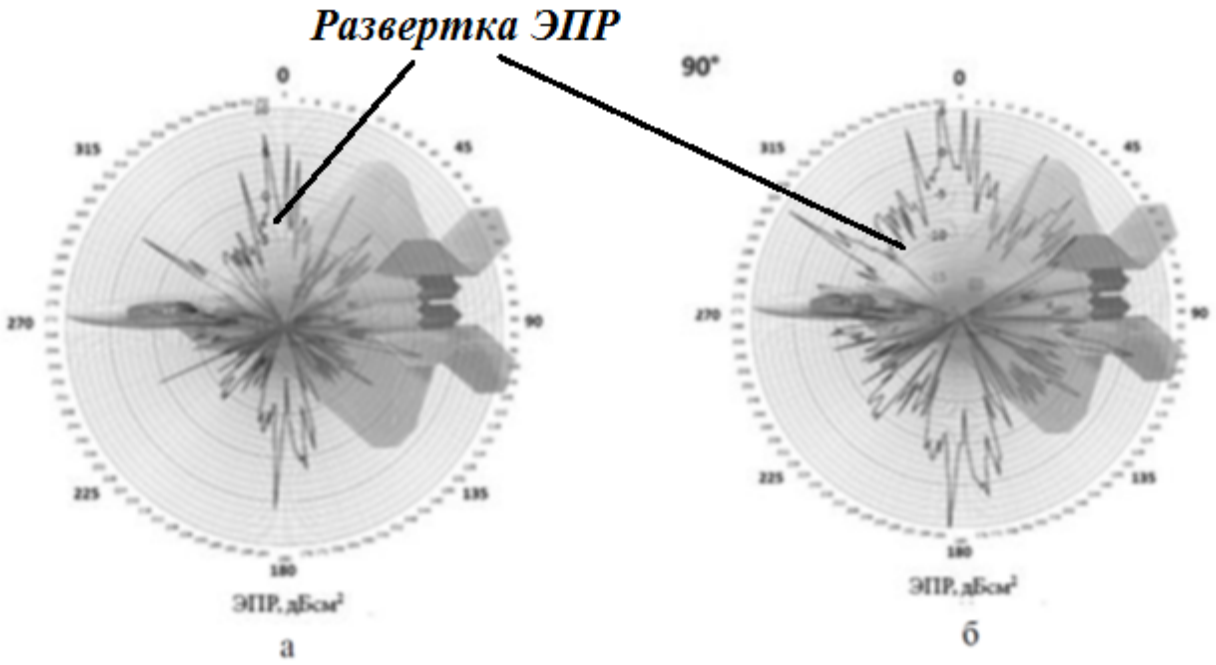



Рис. 5. *а*) круговая развертка ЭПР модели истребителя F-22 “Raptor”;
*б*) увеличенный масштаб

### *Обсуждение*

Учитывая, что на затухание ТГц и ИК излучения влияет достаточно много факторов целесообразно экспериментально определить эффективность широкополосной системы наведения (ШСН) для мутных сред [5, 6]. Эффективность определим, сравнив затухание ТГц и ИК излучения при прохождении мутных

сред. На рис. 6 представлена полученная нами в результате обработки литературных экспериментальных данных концентрационная зависимость затухания излучения ИК и ТГц диапазона. Пылевой заслон создавался бентонитовым порошком, который представляет собой смесь глины, образованной из разложения вулканического пепла и в основном состоящей из монтмориллонита и бейделлита. Авторами использовался бентонит в виде частиц пыли для загрузки камеры. Средний радиус частиц составляет 4,3 мкм. Как видно из рис. 6, поглощением ТГц излучением в мутных песчаных средах по сравнению с поглощением ИК излучения можно пренебречь.

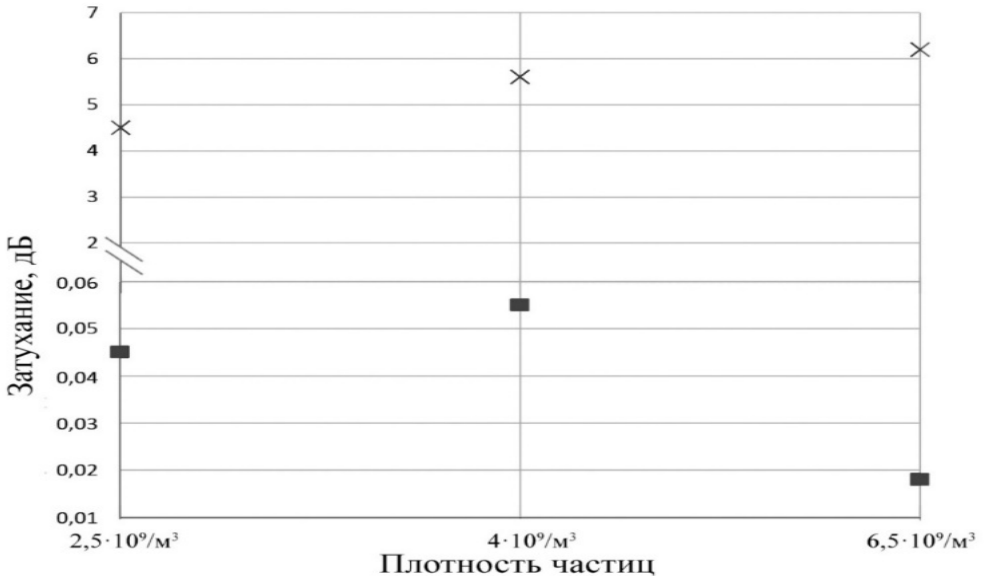



Рис. 6. Эффективность ТГц локаторов при лоцировании в условиях пылевой (бентонитовой) завесы – эксперимент: (X) – ИК излучение (λ= 1,5 мкм, f = 200 ТГц), (■) – ТГц излучение (f = 0,625 ТГц), средний радиус частиц – 4,3 мкм

Уровень эффективности работы ТГц локатора по сравнению с ИК-локатором ясен из рис. 7, где приведена расчетная частотная зависимость отношения затуханий ИК и ТГц диапазонов ($\chi_{ИК}/(\chi_{ТГц}$).

Плотность частиц: $5*10^6$ частиц на кубический сантиметр, радиус частиц 0,2 мкм – расчет. **f**=1 ТГц – точечная линия, **f**= 2 ТГц – штриховая линия, **f**=3 ТГц – штрих пунктирная линия. Расчет выполнен с использованием данных [7].

Данные, приведенные на рис.7, показывают, что при задымлениях ТГц локатор более эффективен, чем ИК локатор. Приведенные данные относятся к отдельным частотам, для многих других частот экспериментальные результаты отсутствуют. Таким образом, существует необходимость получения экспериментальных данных по затуханию ИК и ТГц излучения в атмосфере и мутных средах во всем ТГц диапазоне, где такие данные практически отсутствуют (имеются лишь результаты расчета).

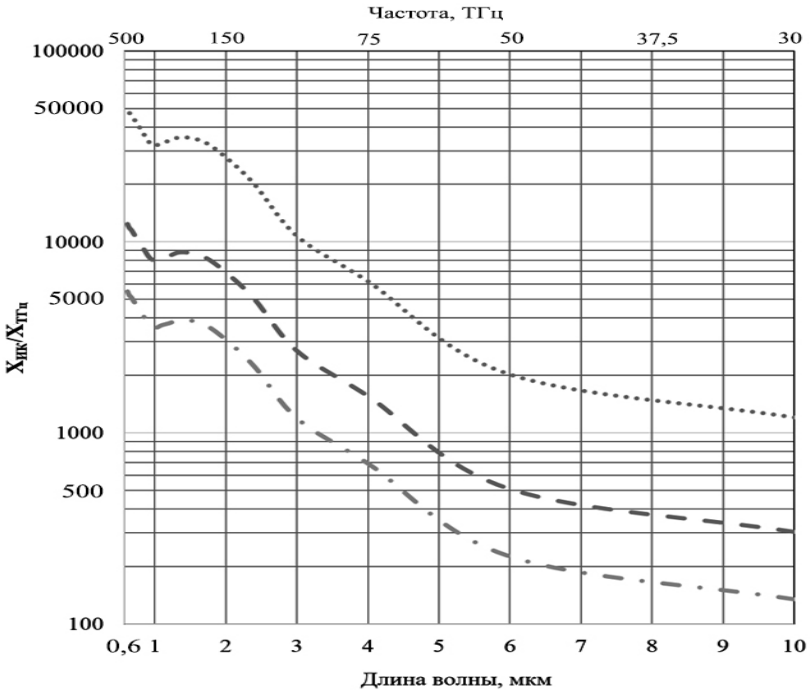



Рис. 7. Сравнительная эффективность ТГц локаторов и локаторов ИК диапазона (1,5 мкм, f = 200 ТГц) при лоцировании в условиях дымовой завесы

В настоящее время в мире ведется интенсивная работа по созданию ТГц локаторов, а, значит, и систем наведения табл. 2.

*Таблица 2*

Область применения ТГц локаторов для тропосферы

| Источники | Тип локатора | Области применения |
|---|---|---|
| [8-11] | Активный | Получение ЭПР сложных электрически крупных тел |
| [12] | Активный | Обеспечение безопасности объектов |
| [13-16] | Активный | Обеспечение безопасности людей, в том числе и на массовых мероприятиях, аэропортах, вокзалах, митингах |

Преимущество ТГц локаторов – возможность работать при наличии пылевых, дымовых завес и тумана, высокая точность, основной недостаток – короткодействие.

Важным преимуществом ИК локаторов и систем наведения является их дальнодействие, поскольку они работают в окнах прозрачности атмосферы табл. 3.

Таким образом, ИК и ТГц локаторы дополняют друг друга. Исходя из этого, разработка широкополосных (ИК-ТГц) систем обнаружения (наведения) является целесообразной табл. 4.

*Таблица 3*

ИК локаторы

| Название ИК локатора | Организация, страна | Диапазон перестройки, нм | Энергия, мДж | Частота повт., Гц | Длит. имп., нс | Ширина линии, $см^{-1}$ | Расходимость, мрад |
|---|---|---|---|---|---|---|---|
| MOPO-HF | Spectra Physics, USA | 440–1 800 | 75 | 10 | 4–6 | 0,075 | – |
| Scan Line-S | Lambda Phusics Inc., USA | 420–2 500 | 150 | 1 000 | 7 | 1 | – |
| Panther | Continium, USA | 410–2 500 | 100 | 10 | 7 | 0,1 | – |
| Mirage 3 000 | Continium, USA | 1 500–4 000 | 10 | 10 | 0,5 | 0,017 | – |
| BBO-3BII | U-Oplaz Technologies Inc., USA | 200–4 000 | 100 | 1–100 | 1–10 | – | – |
| OPO-C | Polytec PI Inc., USA | 205–4 000 | до 150 | 50 | 6–12 | 0,3 | – |
| Vega 200 | Thomson CSF Laser, France | 225–4 000 | 50 | 10 | 10 | 0,2 | – |
| Sunlite EX | Continium, USA | 205 **f**=5 000 | 50 | 7 | 7 | 0,02 | – |
| LT2215 | Lotis TII, Беларусь | 410–2 500 | 40 | 20 | 5–6 | 0,24 | 4–8 |
| OPO ABC | СГГА, Новосибирск, РФ | 1 441–4 240 | до 50 | 25–30 | 10 | 0,6 | 3,3–3,5 |

*Таблица 4*

Обоснование перспективности создания широкополосной (ИК-ТГц) системы наведения – ШСН

| № п/п | Характеристика ШСН | ИК канал | ТГц канал | Прогнозируемое св-во ШСИ |
|---|---|---|---|---|
| 1 | Размер лоцируемого объекта, м | 0,01 м | 0,1 м | 0,1 |
| 2 | Дальнодействие | 10 км | Не установлено, требуются экспериментальные исследования. В отдельных расчетах R ~ 10 км. Известные из открытой печати результаты, ~ 0,1 км | Экспертные оценки - 1 км |
| 3 | Работоспособность в тумане | Нет | Да | Да |

*Окончание табл. 4*

| № п/п | Характеристика ШСН | ИК канал | ТГц канал | Прогнозируемое св-во ШСИ |
|---|---|---|---|---|
| 4 | Работоспособность при дымовой завесе | Нет | Да | Да |
| 5 | Работоспособность при пылевой завесе | Нет | Да | Да |
| 4 | Работоспособность при северном сиянии северного сияния | Да | Да | Да |
| 5 | Работоспособность при региональных конфликтах | Фрагментарно | Фрагментарно | Работоспособно |
| 6 | Работоспособность при антитеррористических операциях | Фрагментарно | Фрагментарно | Работоспособно |
| 7 | Работоспособность при чрезвычайных ситуациях | Фрагментарно | Фрагментарно | Работоспособно |

## *Заключение*

Анализ публикаций и патентов указывает на заметный рост научных прикладных работ, направленных на освоение ТГц диапазона для решения народнохозяйственных и оборонных задач, в заметной степени направленных на использование ТГц излучения в локации.

1. Начиная с 2000 года патентная активность в этой области в странах НАТО, Китае и Японии возрастает практически линейно, в то время как в России подобная тенденция слабо выражена, поскольку число российских патентов и заявок в области перспективных локационных технологий терагерцового диапазона на порядок меньше, чем в США, а также Китае и Японии.

2. Полученные экспериментальные данные по локации в ТГц диапазоне показали принципиальную возможность реализации систем наведения в ТГц диапазоне. Выполненный анализ указывает на необходимость экспериментального исследования затуханию ИК и ТГц излучения в атмосфере и мутных средах (пылевая и дымовая завеса, туман) во всем ТГц диапазоне, что дает возможность разработки широкополосной системы наведения работоспособной при локальных конфликтах, антитеррористических операциях, чрезвычайных ситуациях, сопровождаемых пылевыми и дымовыми завесами, а также работоспособных в тумане и при северном сиянии. Такие ШСН смогут выполнять задачи обнаружения объектов установленными пылевыми и дымовыми завесами, в частности, при для защиты от ИК систем наведения.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Cherevko A.G. Patent activity of developed countries in the terahertz range – Comparative analysis // Proceedings13th International Scientific-Technical Conference on actual problems of electronics APEIE - 2016. - Vol. 1, Part 2. - P. 190-192.

2. Усанов Д.А, Романова Н.В., Салдина Е.А. перспективы и тенденции развития терагерцовых технологий: патентный ландшафт // Экономика науки. – 2017. - Т.3, № 3. - С. 189-202.

3. Михайленко С.Н., Бабиков Ю.Л., Головко В.Ф. Информационно-вычислительная система "Спектроскопия атмосферных газов". Структура и основные функции // Оптика атмосферы и океана. 2005. - Т. 18, № 09. - С. 765-776.

4. Черевко А.Г. и др. Рассеяние терагерцовых волн объектами сложной конфигурации с использованием Новосибирского лазера на свободных электронах // Вестник СибГУТИ. 2016. № 3. – С. 204-214.

5. SuK. etal. Experimental comparison of terahertz and infrared data signal attenuation in dust clouds // Journal of the Optical Society of America A. - 2012. - vol. 29, number 11. - p. 2360.

6. Su K. et al. Experimental comparison of performance degradation from terahertz and infrared wireless links in fog // Journal of the Optical Society of America A. - 2012. - vol. 29, number 2. - p. 179.

7. Jung P. et al. The influence of smoke on the THz imaging // Photonics Letters of Poland. - 2012. - vol. 4, number 3. - p. 94-96.

8. Gente R. et al. Scaled bistatic radar cross section measurements with a fiber-coupled THz time domain spectrometer // 2012 37th International Conference on Infrared, Millimeter, and Terahertz Waves. - 2012. - doi: 10.1109/IRMMW-THz.2012.6380347.

9. Liang L. et al. Broadband and wide-angle RCS reduction using a 2-bit coding ultrathin metasurface at terahertz frequencies // Scientific Reports. - 2016. vol. 6, number 1. - doi: 10.1038/srep39252.

10. Iwaszczuk K., et. al. Terahertz radar cross section measurements // OPTICS EXPRESS. - 2010. - Vol. 18, No. 25. - p. 26399-26408

11. Lui H. et al. Terahertz radar cross-section characterisation using laser feedback interferometry with quantum cascade laser // Electronics Letters. - 2015. - vol. 51, number 22. - p. 1774-1776.

12. Yang Q. et al. Experimental research on vehicle-borne SAR imaging with THz radar // Microwave and Optical Technology Letters. - 2017. - vol. 59, number 8. - p. 2048-2052.

13. Song Q., et. al. Fast continuous terahertz wave imaging system for security // Opt. Commun. - 2009. - vol. 282. no. 10. - pp. 2019–2022.

14. Grajal J. et al. 3-D High-Resolution Imaging Radar at 300 GHz With Enhanced FoV // IEEE Transactions on Microwave Theory and Techniques. - 2015. vol. 63, number 3. - p. 1097-1107.

15. Cooper K. et al. Fast high-resolution terahertz radar imaging at 25 meters // Terahertz Physics, Devices, and Systems IV: Advanced Applications in Industry and Defense. - 2010. – doi: 10.1117/12.850395.

16. Federici J. et al. THz imaging and sensing for security applications—explosives, weapons and drugs // Semiconductor Science and Technology. - 2005. vol. 20, number 7. - p. S266-S280.

УДК 621.752
DOI: 10.33764/2618-981X-2019-9-98-105

# ПОВЫШЕНИЕ ТОЧНОСТИ И ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ОПТИЧЕСКИХ СИСТЕМ ПРИ ПРОВЕДЕНИИ ИЗМЕРЕНИЙ

***Валерик Сергеевич Айрапетян***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, зав. кафедрой специальных устройств инноватики и метрологии, тел. (383)361-07-31, e-mail: v.s.ayrapetyan@sgga.ru

***Георгий Алексеевич Куриленко***
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. К. Маркса, 20, доктор технических наук, профессор кафедры прочности летательных аппаратов, e-mail: teormech@ngs.ru

В работе рассмотрен способ виброизоляции оптических приборов, существенно улучшающий точность измерений. Представлен разработанный термографический метод определения характеристик статической трещиностойкости металлов, позволяющий повысить их достоверность на 30% и тем самым надежность работы оптических систем при проведении измерений.

**Ключевые слова:** защита от вибрации, достоверность измерений, термографический метод, трещиностойкость.

# INCREASE OF ACCURACY AND SAFETY SECURING OF OPTOMECHANICAL DEVICES WHENMEASURING

***Valerik S. Ayrapetyan***
Siberian State University of Geosystems and Technologies, 10, Plahotnogo St., Novosibirsk, 630108, Russia, D. Sc., Head of Department of Special Devices for Innovation and Metrology, phone: (383)361-07-31, e-mail: v.s.ayrapetyan@sgga.ru

***Georgy A. Kurylenko***
Novosibirsk State Technical University, 20, Prospect K. Marx St., Novosibirsk, 630073, Russia, D. Sc., Professor, Department of Strength of Aircraft, e-mail: teormech@ngs.ru

This article examines the vibration-proof devices, essentially improving accuracy of measuring. A new thermographic method for definition of static crack resistance characteristics of material is offered. This method allows define these characteristics more precisely and quickly, increasing the reliable of optomechanical devices.

**Key words:** vibration protection, reliability of measuring, thermographic method, crack resistance.

Современные оптические экспериментальные исследования предъявляют высокие требования к оптико-механическим системам, которые должны обладать достаточной точностью, надежностью и стабильностью работы для обеспечения высокоточных пространственно-временных измерений. Эта проблема особенно актуальна при проведении лидарных измерений в открытой атмосфе-

ре, когда лазерный источник и все оптические элементы располагаются либо на подвижной платформе, либо на летательном аппарате. В этом случае оптико-механические приборы и лазеры, используемые для метрологических измерений, эксплуатируются в экстремальных условия при значительных внешних нагрузках и предъявляемые к ним требования не снижаются.

Решение этой проблемы следует рассматривать в двух аспектах.

Первый аспект – технологический, требующий виброзащиты оптической системы при производстве от фоновой вибрации производственных и лабораторных помещений.

Второй аспект – эксплуатационный, требующий, с одной стороны, обеспечения прочностной надежности отдельных узлов и в целом оптической системы, а с другой стороны, достаточной точности проводимых измерений в условиях вибрационных и других воздействий при их эксплуатации.

В настоящее время разработано множество различных конструкций виброзащитных устройств, каждое из которых имеет свою область применения [1–3]. Об универсальном устройстве пока говорить рано, но, как отмечают практически все авторы, самой актуальной остается проблема повышения качества виброзащиты.

В [1, 2] разработана виброзащитная платформа с упругим элементом (рис. 1), позволяющая получить существенное продвижение в решении этой проблемы.

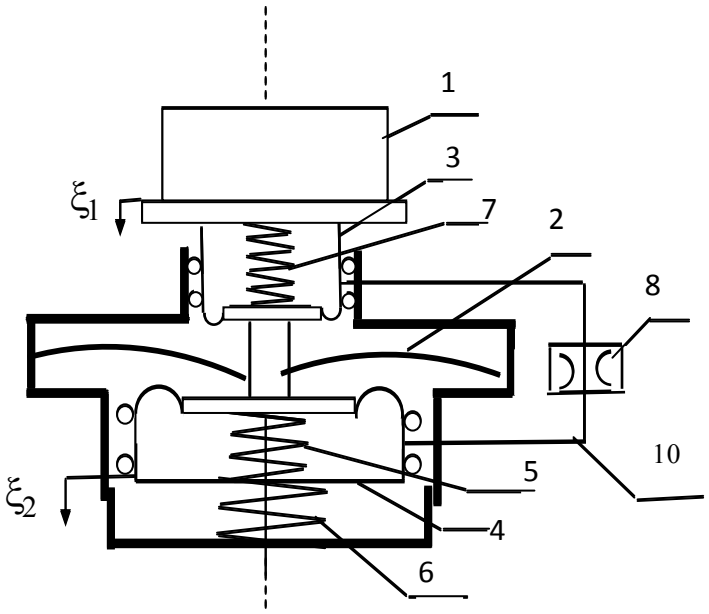



Рис. 1. Виброзащитная платформа

Защищаемый прибор 1 опирается на подвес 2 в виде продольно-сжатой балки (рессоры) квазинулевой жесткости и пружину 6 через гидроцилиндры 3 и 4. Полости этих гидроцилиндров соединяются каналом 10 со встроенным дроссе-

лем 8. Цилиндро-поршневые пары 3 и 4 содержат также упругие элементы 7 и 5 вспомогательного нагружения. Расчетное положение прибора (рабочую точку) устанавливают для создания распорного усилия в рессоре 2, при котором она будет иметь квазинулевую жесткость. Достигается это варьированием натяга пружины 6.

Платформа работает следующим образом. При увеличении, например, веса прибора 1 повышается давление в гидроцилиндре 3, и начинается переток жидкости в гидроцилиндр 4, в результате чего увеличивается натяг пружины 6. Благодаря этому рабочую точку подвеса 2 можно удержать на прежнем уровне. Время перетекания жидкости при этом должно быть существенно больше периода колебаний прибора 1 на подвесе 2 и регулируется величиной проходного сечения канала дросселя 8 [4].

В качестве обобщенной координаты выберем координату $\xi_1$, отсчитываемую от положения равновесия защищаемого прибора 1 с массой $m$. $\xi_2$– координата, определяющая положение цилиндра 4.

Рассмотрим свободные колебания системы с нелинейной упругой характеристикой рессоры. Для первоначальной настройки рабочей точки к массе $m$ присоединяем груз массой $m_1$. Тогда уравнение движения объекта 1 запишется так [5]

$$(m + m_1)\ddot{\xi}_1 = -k_1\xi_м - k_3\xi_м^3 - c_3\xi_2 + m_1 g, \qquad (1)$$

где $k_1$, $k_3$ – коэффициенты упругой характеристики рессоры 2,

$\xi_м$ – ее максимальный прогиб,

$c_3$ – коэффициент жесткости пружины 6.

Учтем также перемещение цилиндра 4 отдельно и этого цилиндра вместе с поршнем при условии, что массой поршней и цилиндров пренебрегаем:

$$\left.\begin{aligned} P_2S_2 &= c_3\xi_2 + c_2(\xi_2 - \xi_м) \\ P_1S_1 &= k_1\xi_м + c_3\xi_2 - c_1(\xi_1 - \xi_2), \end{aligned}\right\} \qquad (2)$$

где $c_1$, $c_2$ коэффициенты жесткости вспомогательных пружин 7 и 5;

$S_1$, $S_2$ – соответственно площади верхнего, нижнего цилиндров;

$P_1$, $P_2$ – соответственно давления жидкости в верхнем и нижнем цилиндрах.

Одним из важных показателей данной виброзащитной системы является время возвращения рабочей точки рессоры в начальное положение. Из решения уравнений (1) и (2) на рис. 2 показан процесс затухания свободных колебаний объекта и рессоры при использовании в качестве жидкости керосина, у которого динамический коэффициент вязкости $\mu = 1{,}5 \cdot 10^{-3}$ Пас.

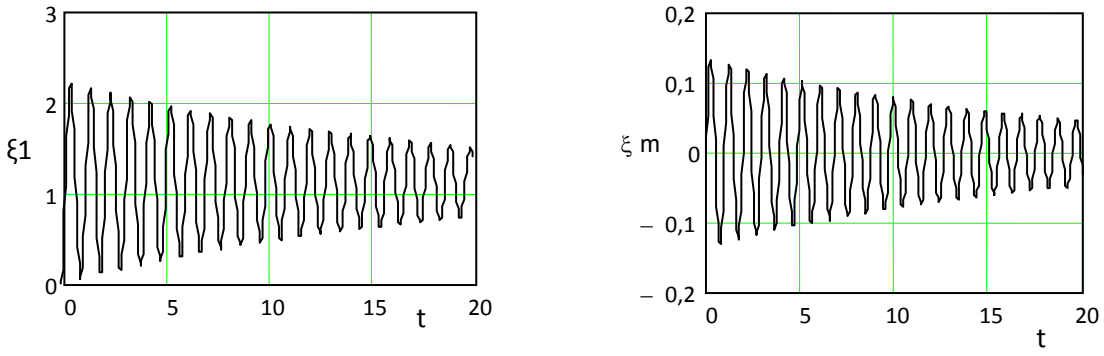



Рис. 2. Затухание свободных колебаний (керосин)

Параметры системы:

$$S_2 / S_1 = 5, \quad c_3 = 22 \cdot 10^3 \text{ н/м}, \; k_1 = -17 \cdot 10^3 \text{ Н/М}, \quad m = 100 \text{ кг}, \quad m_1 = 5 \text{ кг}.$$

Из рис. 2 видно, что колебательный процесс объекта и рессоры около равновесного положения длится более 20 сек. В первые секунды объект отклоняется от своего нового начального положения около 1 см. В это же время рессора получает небольшое перемещение около 0,1 см, так как процесс перетекания жидкости начинается сразу.

Затухание колебаний можно ускорить если увеличить коэффициент вязкости. На рис. 3 показан затухающий процесс свободных колебаний, где в качестве жидкости взят скайдрол (авиационная рабочая жидкость) с коэффициентом вязкости $\mu = 1{,}16 \cdot 10^{-2}$ Пас.

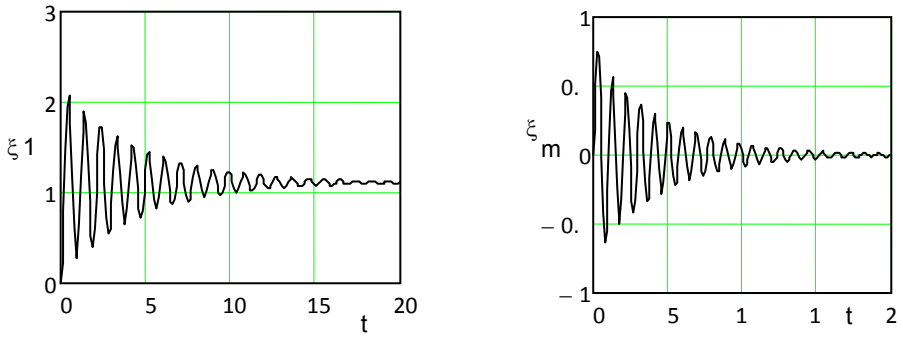



Рис. 3. Свободные колебания (скайдрол)

Из рис. 3 видно, что процесс возвращения рабочей точки рессоры носит также колебательный характер, но затухает около 15 сек. При этом первое отклонение объекта почти не изменилось, а рессора получает больший прогиб в сравнении с предыдущим, около 0,6 см.

Исследовано также затухание свободных колебаний при использовании в качестве рабочих жидкостей трансформаторного и оливкового масел. Показано, что с увеличением коэффициента вязкости время возвращения рессоры в начальное положение возрастает и начальная амплитуда объекта практически на меняется.

Для исследования вынужденных колебаний данной системы придадим уравнению (1) вид

$$\ddot{\xi}_1 = -c_{11}\xi_м - c_{12}\xi_1 - c_{13}\xi_м^3 - 2n\xi_1 - A_e\dot{\omega}^2\sin(\omega t), \qquad (3)$$

где $c_{11} = \frac{k_1 + c_3\left(1-\frac{S_1}{S_2}\right)}{m+m_1}$, $c_{12} = \frac{c_3 S_1}{S_2(m+m_1)}$, $c_{13} = \frac{k_3}{m}$.

В уравнении (3) учитывается нелинейность упругой характеристики рессоры и дополнительное вязкое демпфирование, в котором учитывается нелинейность упругой характеристики рессоры и дополнительное вязкое демпфирование.

Рассматривается кинематическое воздействие с амплитудой основания $A_e$ и частотой $\omega$. Расчет проведен при амплитуде колебаний основания $A_e = 2{\cdot}10^{-2}м$ и коэффициентах $n = 2{,}5\frac{1}{c}$, $k_3 = 2\cdot 10^7\,\frac{Н}{м^3}$. На рис. 4 показан рассчитанный график зависимости коэффициента передачи (КП) от частоты колебаний основания $\nu$, из которого видно, что для КП получены вполне приемлемые значения. Так при резонансной частоте $\nu = 1\,Гц$ КП = 1,6, а при $\nu > 5$ Гц перетекания жидкости нет и цилиндры 3 и 4 вместе с объектом будут двигаться как одно целое.

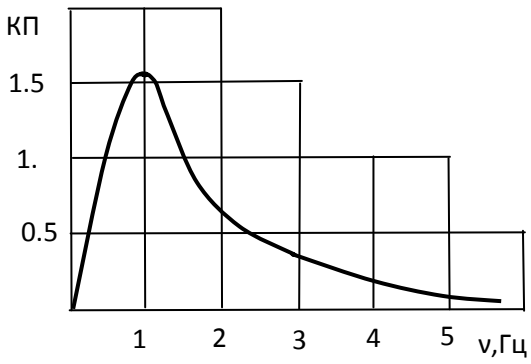



Рис. 4. Коэффициент передачи при кинематическом воздействии

Рассмотрим весьма актуальный случай – ударную нагрузку. Пусть, по основанию нанесен удар силой $F_0$ = 290 *Н*с длительностью Т = 0,1 сек. Уравнение (3) этом случае запишется так

$$\left.\begin{aligned} m\ddot{\xi}_1 &= -k_1\xi_м - k_3\xi_м^3 - c_3\xi_2 - b\dot{\xi}_1 + F_0\cdot\sin\frac{\pi T}{t}\ , \quad при\ t < T \\ m\ddot{\xi}_1 &= -k_1\xi_м - k_3\xi_м^3 - c_3\xi_2 - b\dot{\xi}_1, \text{ при } t \geq T\ , \end{aligned}\right\} \qquad (4)$$

Из рис. 5 видно, что в этом случае колебания затухают практически за один период. Движение объекта и рессоры почти синхронно.

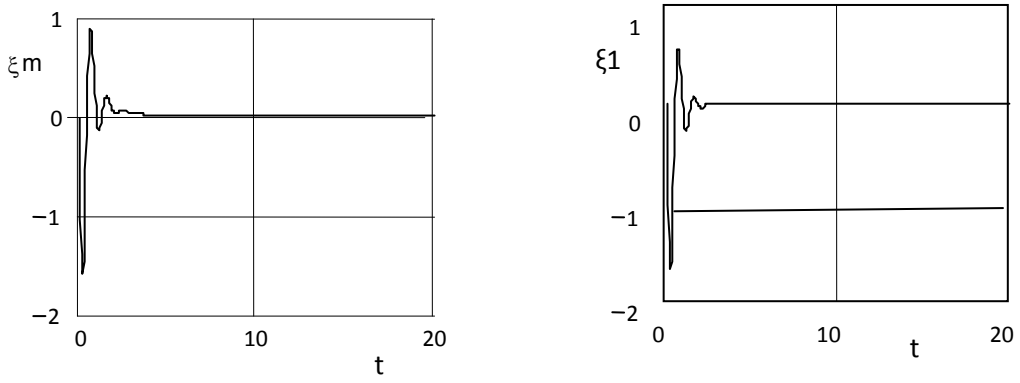



Рис. 5. Затухание колебаний при ударе

Определенный интерес представляет аналогичное исследование виброзащитной подвески с электромеханическими элементами управления.

На рис. 6 показана такая подвеска, где 1 – защищаемый объект, 2 – нелинейно-упругий элемент, 3 – регулировочная пружина с постоянной жесткостью $C_2$, натягом которой можно компенсировать изменение веса объекта. Для этого конец пружины перемещают механизированным приводом 4, используя показания датчика положения объекта.

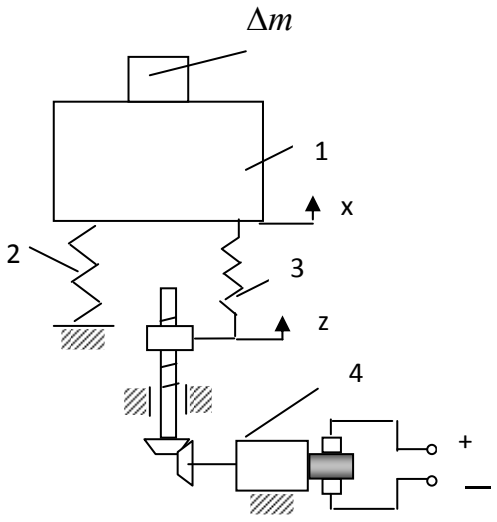



Рис. 6. Схема виброзащитной подвески
с электромеханическим управлением

Рассмотрим уравнение вынужденных колебаний объекта массы $m$, например, при увеличении его массы на $\Delta m$ и перемещении конца пружины 3 по закону $z = \mathrm{v} \cdot \mathrm{t}$ ( V – скорость перемещения).

$$\ddot{x} + k_1^2 x + k_3 x^3 + k_2 z + 2n\dot{x} - G = A_e \omega^2 \sin \omega t \qquad (5)$$

где $k_1, k_3$ –коэффициенты нелинейной упругой характеристики,

$k_2$– коэффициент упругой характеристики регулировочной пружины,

$n$ – коэффициент демпфирования,

$$G = \Delta m g / (m + \Delta m).$$

Интегрируем (5) при:

$$k_1 = 6{,}28 \text{ с}^{-1},\ k_2 = 181{,}1 \text{ с}^{-2},\ k_3 = 3{,}96 \text{ см}^{-2}\text{с}^{-2},\ n = 3 \text{ с}^{-1},$$

$$m = 100 \text{ кг},\ \Delta m = 20 \text{ кг},\ A_e = 2 \text{ см},\ \omega = 2 \cdot \pi \cdot \nu = 3{,}142 \text{ с}^{-1},\ \text{v} = 0{,}4 \text{ см/с}.$$

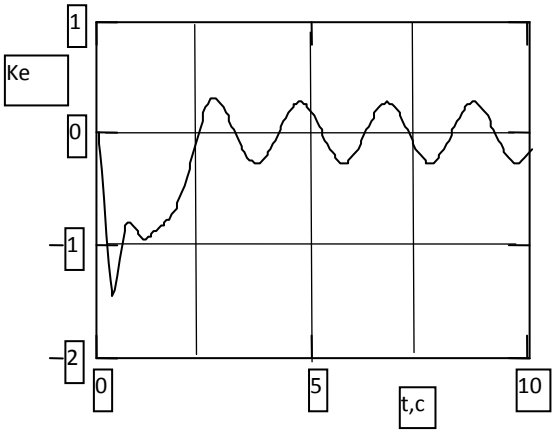



Рис. 7. Зависимость относительного перемещения объекта с добавочной массой от времени

На рис. 7 показана зависимость относительного перемещения $K_e$ объекта с добавочной массой от времени. Процесс возвращения рабочей в номинальное состояние в данном случае занял около 3 с. Конец регулировочной пружины достаточно было переместить на 0,92 см.

### *Заключение*

Подводя итог, следует отметить, что описанные виброзащитные устройства с автоматическим поддержанием рабочей точки подвеса на заданном уровне апробованы в лабораторных условиях [6] и показали достаточно высокую эффективность защиты без энергопотребления в системе управления.

Считаем, что эти устройства могут существенно улучшить виброизоляцию оптических систем, используемых для проведения метрологических измерений, и тем самым повысить точность измерений.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Kurilenko G.A., Yur’ev G.S., Rykov A.A. Synthesis of an Active Vibrational Protection System // Russian Engineering Research. 2014. №7**.** P. 440-443.

2. Kurilenko G.A., Ayrapetyan V.S. Determination of the Fracture Toughness of Optomechanical Devices // OpticsandPhotonicsJournal.2016. №6**.** P 298-304.

3. ХелланК. Введение в механику разрушения. Пер. с англ. / Под ред. Морозова Е.М. М., 1988. 364 с.

4. Ковчик С.В., Морозов Е.М. Механика разрушения и прочность материалов. Справочное пособие. / Под.ред. Панасюка В.В. Киев: Наукова думка, 1988. Т.3. 435 с.

5. ГОСТ 25.506-85. Расчеты и испытания на прочность. Методы механических испытаний металлов. Определение характеристик трещиностойкости (вязкости разрушения) при статическомнагружении // – М: Изд. стандартов, 1985. 61 с.

6. Куриленко Г.А., Пшеничный А.Б. Способ определения трещиностойкости материалов // А.с. № 1820278. Бюл. изобр.1990. №21. С. 72.

7. Базаров И.П.Термодинамика. – М.: Высшая школа, 1983. 344 с.

УДК 623.45
DOI: 10.33764/2618-981X-2019-9-106-115

# ЗАДАЧИ ПРОНИКАНИЯ НЕДЕФОРМИРУЕМОГО УДАРНИКА В ПРЕГРАДУ

***Евгений Владимирович Проскуряков***
Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, кандидат технических наук, доцент, профессор кафедры, тел. (383)332-50-45, e-mail: saper67@mail.ru

***Михаил Васильевич Сорокин***
Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, кандидат технических наук, доцент, преподаватель, тел. (383)332-50-45, e-mail: mv_sorokin@ngs.ru

***Александр Иванович Пошехонов***
Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, курсант 4-го курса батальона (войсковой разведки) тел. (999)468-72-42

В данной работе представлены инженерные модели проникания недеформируемых ударников в преграды: дерево, грунт, бетон, сталь, воду. В качестве недеформируемых ударников использованы: пуля винтовки снайперской специальной ВСС, бетонобойный артиллерийский снаряд калибром 152 мм, боевая часть бетонобойного неуправляемого авиационного реактивного снаряда С-8БМ калибром 80 мм, бронебойный снаряд калибром 30 мм, пуля автомата подводного специального АПС калибром 5,66 мм, пуля автомата двухсредного специального АДС калибром 5,45 мм.

Предполагается, что силу сопротивления среды можно представить в виде суммы трех сил: силы динамического сопротивления, пропорциональной квадрату скорости проникания, силы вязкости среды, пропорциональной скорости проникания и силы статического сопротивления среды, которая не зависит от скорости проникания.

Выполнены расчеты проникания типовых ударников, которые удовлетворительно согласуются с эмпирическими формулами. Перечисленные модели необходимы для решения военно-прикладных задач проникания боеприпасов в различные преграды.

**Ключевые слова:** проникание, преграда, пуля, артиллерийский снаряд, реактивный снаряд, бронебойный снаряд, бетонобойный снаряд.

# PROBLEMS OF PENETRATION OF AN UNDEFORMABLE DRUMMER INTO AN OBSTACLE

***Evgeny V. Proskuryakov***
The Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Ph. D., Associate Professor, Professor of Department, phone: (383)332-50-45, e-mail: saper67@mail.ru

***Mikhail V. Sorokin***
The Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Ph. D., Associate Professor, Lecturer, phone: (383)332-50-45, e-mail: mv_sorokin@ngs.ru

***Aleksandr I. Poshekhonov***
The Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Cadet 4 Course Battalion of the Army Intelligence, phone: (999)468-72-42

This paper presents engineering models for the penetration of undeformable drummers into obstacles: wood, concrete, steel and water. As undeformable drummers used: special sniper rifle bullet VSS, concrete artillery shell caliber of 152 mm, the warhead of a concrete-piercing unguided aviation missile S-8BM caliber of 80 mm, armor-piercing shell of 30 mm caliber, bullet of a submarine special APS submachine gun with a caliber of 5,66 mm, bullet of submachine gun special two-mediums ADS with a caliber of 5,45 mm.

It is assumed that the resistance force of medium can be represented as the sum of three forces: dynamic drag forces proportional to the square of penetration rate, the velocity of the medium in proportion to the penetration rate and the strength of the static resistance of the medium, which is independent of the penetration rate.

Penetration calculations of typical drummers were performed that are in satisfactory agreement with empirical formulas. The listed models are necessary for solving military-applied tasks of penetrating ammunition into obstacles.

**Key words:** penetration, obstacle, bullet, artillery shell, aviation missile, armor-piercing shell, concrete projectile.

## *Введение*

При проникании ударника в сплошную среду его движение описывается законом Ньютона: $m \cdot dV/dt = -F$, где $m$ – масса ударника, $V$ – его скорость, $t$ – время, $F$ – сила сопротивления среды. Начальные данные для решения дифференциального уравнения: при $t = 0$, $x = 0$, $dx/dt = V_0$.

Здесь $x$ – перемещение ударника, $V_0$ – начальная скорость ударника.

Предполагается, что $F$ можно представить в виде суммы трех сил:

$$F = S\cdot(A\cdot V^2 + B\cdot V + C),$$

где $S$ – площадь поперечного сечения ударника, $F_1=S\cdot A\cdot V^2$ – сила динамического сопротивления, пропорциональная квадрату скорости проникания $V$;

$F_2=S\cdot B\cdot V$ – сила вязкости среды, пропорциональная скорости проникания;

$F_3$ $F=S\cdot C$ – сила статического сопротивления среды, которая не зависит от скорости проникания.

Эта зависимость была предложена Покровским [2-3] для описания следующих преград: грунт $(A = 0, C = 0, B \neq 0)$, бетон $(B = 0, A \neq 0, C \neq 0)$, сталь $(A = 0, B = 0, C \neq 0)$, вода и воздух $(B = 0, C = 0, A \neq 0)$ и др. При этом свойства материалов существенно зависят от скорости проникания $V$.

## *Методы и материалы*

Рассмотрим следующие задачи [3].

*Задача 1.* Пуля калибром $d = 9$ мм и массой $m = 16$ г (винтовка ВСС) подлетает к преграде со скоростью $V_0 = 110$ м/с [1-3, 7, 9-10, 12, 15, 18, 19-20].

Сила статического сопротивления преграды

$$F = S \cdot \sigma \qquad (1.1)$$

где $S = \pi \cdot d^2/4$, $\sigma$ = 6 кг/мм$^2$= 60 МПа (дерево).

Найти глубину $h$ проникания пули в преграду.

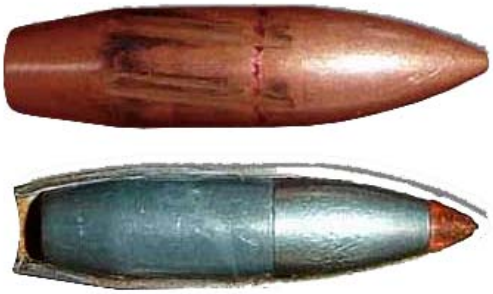


Рис. 1. Пуля винтовки ВСС

*Решение.* Ускорение пули:

$$a = F / m \tag{1.2}$$

$$a = \pi \cdot d^2 \cdot \sigma / (4 \cdot m) \tag{1.3}$$

$a = 250 \cdot 10^3$ м/с$^2$ (25 тыс. g).

Пуля движется в преграде равнозамедленно. Из кинематики равнозамедленного движения: $h = V_0^2/(2 \cdot a)$; $h$ = 24 мм.

Деревянная доска толщиной 1 дюйм (около 25 мм) используется для оценки действия поражающего элемента (пули) по живой силе (ЖС) в качестве эквивалента.

*Задача 2.* Пуля массой $m$ = 16 г и калибром $d$ = 9 мм вылетает из винтовки ВСС с начальной скоростью $V_0$ = 280 м/с [1-3, 7, 9-10, 12, 15, 18, 19-20].

Для поражения живой силы (ЖС) противника необходима кинетическая энергия пули $E$ = 100 дж. Плотность воздуха $\rho_B$ = 1,2 кг/м$^3$, баллистический коэффициент пули $C_x$ = 1.

Найти предельное расстояние $l_n$ (интервал) поражения ЖС (убойный интервал пули). Результаты расчета сравнить с тактико-техническими характеристиками (ТТХ) винтовки $l_n$ = 400 м.

*Решение.* Запишем уравнение движения пули и проинтегрируем его:

$$m \cdot \frac{dV}{dt} = -C_x \cdot S \cdot \frac{\rho_B \cdot V^2}{2}; \quad \frac{dV}{V} = -\frac{1}{2 \cdot m} \cdot C_x \cdot \rho_B \cdot S \cdot dx;$$

$$m \cdot \frac{dV}{dx} = -\frac{1}{2} \cdot C_x \cdot S \cdot \rho_B \cdot V; \quad \frac{dV}{V} = -\frac{1}{2 \cdot m} \cdot C_x \cdot \rho_B \cdot S \cdot dx;$$

$$\int_{V_0}^{V_n} \frac{dV}{V} = \frac{1}{2 \cdot m} \cdot S \cdot \rho_B \cdot \int_0^{l_n} dx;$$

$$l_n = \frac{2 \cdot m}{C_x \cdot S \cdot \rho_B} \cdot \ln \frac{V_0}{V_П} \ , \text{ где } S = \pi \cdot D^2 / 4.$$

Пусть $C_x$ = 1; $\rho_B$ = 1,2 кг/м$^3$, $S$ = 0,71 · 10$^{-3}$ м$^2$; $V_0$ = 280 м/с; $V_к$ = 110 м/с. Тогда $l_П$ = 419 м. Результаты расчетов согласуются с данными ТТХ.

*Задача 3.* Бетонобойный артиллерийский снаряд калибром $D$ = 152 мм имеет массу $m$ = 40 кг и скорость у преграды $V_0$ = 400 м/с [1-3, 5, 16].

Найти глубину проникания $h_П$ снаряда дальнобойной формы в грунт (песок). Сила сопротивления преграды: $F = D^2 \cdot V_0 / k$. Для песка $k_П$ = 5,9 · 10$^{-6}$ (снаряд дальнобойной формы, все параметры в системе СИ).

Рис. 2. Бетонобойный артиллерийский снаряд калибром 152 мм

*Решение.* Уравнение движения снаряда в преграде:

$m \cdot dV/dt = -F$; $m \cdot dV/dt = -D^2 \cdot V / k$; $m \cdot dV = -D^2 \cdot V \cdot dt / k$; $V \cdot dt = dx$,

$m \cdot dV = -D^2 \cdot dx / k$.

После интегрирования получим: $h = k \cdot m \cdot V_0 / D^2$ (эмпирическая Березанская формула).

Глубина проникания в грунт (песок): $h_П$ = 4,2 м.

*Задача 4.* Боевая часть (БЧ) бетонобойного неуправляемого авиационного реактивного снаряда (НАР С-8БМ) калибром $D$ = 80 мм имеет массу $m$ = 7,4 кг и начальную скорость $V_0$ = 450 м/с [1-3, 7, 9-10, 12, 15, 18, 19-20].

Сила сопротивления преграды: $F = \pi \cdot D^2/4 \cdot (H_д + k \cdot \rho_п \cdot V^2)$.

Динамическая твердость бетона $H_д$ = 8 · 10$^7$ Па; плотность бетона $\rho_п$ = 2000 кг/м$^3$; коэффициент формы снаряда $k$ = 0,5.

Найти глубину $h_Б$ проникания снаряда в бетон.

Рис. 3. НАР С-8БМ

*Решение.* Обозначим: $C = H_д$; $A = k \cdot \rho_п$. Тогда: $F = \pi \cdot D^2 / 4 \cdot (A \cdot V^2 + C)$.

Рассмотрим дифференциальное уравнение движения снаряда в бетоне: $m \cdot dV/dt = -\pi \cdot D^2 / 4 \cdot (A \cdot V^2 + C)$. В уравнении (1) произведем замену переменной $t$ на переменную $x$. После интегрирования получим формулу (2) для глубины проникания $h_Б$ (эмпирическая формула Забудского).

Глубина проникания в бетон: $h = 0{,}9$ м.

$$\frac{dV}{V^2 + C/A} = -\frac{\pi D^2 A}{4m} dt\,; \quad \frac{2VdV}{V^2 + C/A} = -\frac{\pi D^2 A}{2m} dx \tag{4.1}$$

$$\int_{V_0}^{0} \frac{2VdV}{V^2 + C/A} = -\frac{\pi D^2 A}{2m} \int_0^h dx \tag{4.2}$$

$$\ln(C/A) - \ln\left(V_0^2 + C/A\right) = -\frac{\pi D^2 A}{2m} h \tag{4.3}$$

$$h = \frac{2m}{\pi A D^2} \ln\left(1 + V_0^2\, A/C\right);\; h = \frac{2m}{\pi D^2 k p_n} \ln\left(1 + k p_n V_0^2 \,/ H_\partial\right) \tag{4.4}$$

*Задача 5.* Бетонобойный артиллерийский снаряд калибром $D$ = 152 мм имеет массу $m = 40$ кг и скорость у преграды $V_0 = 400$ м/с [4, 6, 8, 11, 13-14, 17]. Сила сопротивления преграды: $F = \pi \cdot D^2/4 \cdot (H_д + k \cdot \rho_п \cdot V^2)$. Динамическая твердость бетона $H_д = 8 \cdot 10^7$ Па; плотность бетона $\rho_п = 2000$ кг/м$^3$; коэффициент формы снаряда $k = 0{,}5$.

Найти глубину $h_Б$ проникания снаряда в бетон.

*Решение* аналогично задаче 3. По формуле (2): $h = 1{,}2$ м.

*Задача 6.* Имеется бронебойный снаряд [3] калибром $D$ = 30 мм и массой $m = 0{,}4$ кг [4, 6, 8, 11, 13-14, 17].

Найти скорость снаряда $V_0$ для пробития стальной преграды толщиной $h = 40$ мм. Сила сопротивления стальной преграды: $F = S \cdot C_1 \cdot (h / D)^{0,5}$, где $S = \pi \cdot D^2 /4$, $C_1 = 16 \cdot 10^8$ (в системе СИ).

Рис. 4. Бронебойный снаряд калибром 30 мм (вверху)
и его бронебойный сердечник (внизу)

*Решение.* Уравнение движения снаряда в прегра де:
$m \cdot dV/ d\,t = -F$; $m \cdot dV/ d\,t = -C_1 \cdot (h / D)^{0,5} \cdot \pi \cdot D^2 /4$;
$m \cdot dV = -C_1 \cdot (h / D)^{0,5} \cdot \pi \cdot D^2 \cdot d\,t /4$.
Умножим обе части уравнения на $V$:
$m \cdot V \cdot dV = -C_1 \cdot (h / D)^{0,5} \cdot \pi \cdot D^2 \cdot V \cdot d\,t /4$; с учетом: $V \cdot d\,t = dx$, получим:
$m \cdot V \cdot dV = = -C_1 \cdot (h / D)^{0,5} \cdot \pi \cdot D^2 \cdot dx /4$. Проинтегрируем это уравнение и получим формулу (эмпирическая формула Жакоб де Марра):

$$V_0 = \left( \frac{\pi \times C_1}{2} \right)^{0,5} \frac{D^{0,75} \times h^{0,5}}{m^{0,5}} = 770\,м/с\,.$$

*Задача 7.* Пуля для подводной стрельбы из автомата АПС калибром $D$ = 5,66 мм имеет массу $M_0$ = 20 г. На глубине $h$ = 5 м начальная скорость пули равна $V_0$ = 245 м/с, интервал поражения пули составляет $l_5$ = 30 м. Плотность воды $\rho$ = 1000 кг/м$^3$. Критерий поражения ЖС считать в виде энергии поражения $E_n$ = 100 дж.

Определить интервал поражения пули $l_{20}$ на глубине $h$ = 20 м и сравнить с экспериментом ($l_{20}$ = 20 м).

Рис. 5. Патрон автомата АПС

*Решение.* Скорость поражения пули рассчитывается по формуле $V_n = (2 \cdot E_n /m)^{0,5}$ и составляет $V_n$ = 112 м/с [1-3, 7, 9-10, 12, 15, 18, 19-20]. Рассмотрим дифференциальное уравнение (1) движения пули в воде на глубине 5 метров, гидростатическим давлением можно пренебречь.

$$M_0 \times \frac{dV}{dt} = -k \times S \times \frac{p_\beta \times V^2}{2} \tag{7.1}$$

$$\frac{dV}{dt} = \frac{dV}{dx} \times \frac{dx}{dt} = \frac{dV}{dx} \times V \tag{7.2}$$

$$M_0 \times \frac{dV}{dx} = -\frac{1}{2} \times k \times S \times p_\beta \times V \tag{7.3}$$

$$\int_{V_0}^{V_n} \frac{dV}{V} = \frac{k}{2 \times M_0} \times S \times p_\beta \times \int_0^{l_n} dx \tag{7.4}$$

$$\ln V_n - \ln V_0 = \frac{k \times S \times p_\beta \times l_n}{2 \times M_0} \tag{7.5}$$

$$l_n = \frac{8 \times M_0}{k \times \pi \times D^2 \times p_\beta} \times \ln \frac{V_0}{V_n} \tag{7.6}$$

$$k = \frac{8 \times M_0 \times \ln(V_0 / V_n)}{l_n \times \pi \times D^2 \times p_\beta} \tag{7.7}$$

Произведем замену переменной $t$ на переменную $x$ в уравнении (2). После интегрирования получим формулу для убойного интервала пули $l_n$, позволяющую определить по формуле (3) коэффициент лобового сопротивления воды $k = 0{,}04$.

Рассмотрим движение пули на глубине 20 м. Сила сопротивления воды: $F = \pi \cdot D^2/4 \cdot (P + k \cdot \rho_B \cdot V^2/2)$, здесь $P$ – статическая составляющая силы сопротивления. Обозначим: $A = k \cdot \rho_B/2$. Тогда: $F = \pi \cdot D^2 / 4 \cdot (A \cdot V^2 + P)$. Дифференциальное уравнение движения пули в воде на большой глубине имеет вид:

$$M_0 \frac{dV}{dt} = -\frac{\pi \times D^2}{4}\left(A \times V^2 + P\right) \tag{7.8}$$

$$\frac{dV}{V^2 + P/A} = -\frac{\pi \times D^2 \times A}{4 \times M_0} dt \tag{7.9}$$

$$\frac{2 \times V \times dV}{V^2 + P/A} = -\frac{\pi \times D^2 \times A}{2 \times M_0} dx \tag{7.10}$$

$$\int_{V_0}^{V_\Pi} \frac{2 \times V \times dV}{V^2 + P/A} = -\frac{\pi \times D^2 \times A}{2 \times M_0} \int_0^{l_\Pi} dx \tag{7.11}$$

$$\ln\left(V_\Pi^2 + P/A\right) - \ln\left(V_0^2 + P/A\right) = -\frac{\pi \times D^2 \times A}{2 \times M_0} l_\Pi \tag{7.12}$$

Если $P/\left(AV_\Pi^2\right) \approx 0$, то

$$\ln \frac{V_0^2\left[1 + P/\left(AV_0^2\right)\right]}{V_\Pi^2\left[1 + P/\left(AV_\Pi^2\right)\right]} \approx \ln \frac{V_0^2}{V_\Pi^0} = 2 \ln \frac{V_0}{V_\Pi} \tag{7.13}$$

$$l_\Pi \approx \frac{2 \times M_0}{\pi \times A \times D^2} 2 \ln \frac{V_0}{V_\Pi} \tag{7.14}$$

$$l_\Pi \approx \frac{8 \times M_0}{\pi \times k \times p_\beta \times D^2} \times \ln \frac{V_0}{V_\Pi} \tag{7.15}$$

При малых значениях $P$ формула (6) переходит в (3). Пусть $h = 20$ м, тогда $P = \rho \cdot g \cdot h = 2 \cdot 10^5$ Па, $l_П \approx 19$ м.

*Задача 8.* Пуля для подводной стрельбы из автомата АДС калибром $D$ = 5,45 мм имеет массу $M_0$ = 16 г. На глубине 5 м начальная скорость пули равна $V_0$ = 333 м/с, убойный интервал пули составляет $l_5$ = 25 м. Плотность воды $\rho_B$ = 1000 кг/м$^3$. Критерий поражения ЖС считать в виде убойной энергии поражения $E_n$ = 100 дж.

Определить убойный интервал пули $l_{20}$ на глубине 20 м.

$$M_0 \times \frac{dV}{dt} = -k \times S \times \frac{p_{\beta \times V^2}}{2} \tag{8.1}$$

$$\frac{dV}{dt} = \frac{dV}{dx} \times \frac{dx}{dt} = \frac{dV}{dx} \times V \tag{8.2}$$

$$M_0 \times \frac{dV}{dx} = -\frac{1}{2} \times k \times S \times p_\beta \times V \tag{8.3}$$

$$\int_{V_0}^{V_n} \frac{dV}{V} = \frac{k \times S \times p_\beta}{2 \times M_0} \times \int_0^{l_n} dx \tag{8.4}$$

$$\ln V_n - \ln V_0 = \frac{k \times S \times p_\beta \times l_n}{2 \times M_0} \tag{8.5}$$

$$l_n = \frac{2 \times M_0}{k \times S \times p_\beta} \times \ln \frac{V_0}{V_n} \tag{8.6}$$

$$k = \frac{2 \times M_0 \times \ln(V_0 / V_n)}{l_n \times S \times p_\beta} \tag{8.7}$$

Рис. 6. Патрон автомата АДС

*Решение.* Убойная скорость поражения пули рассчитывается по формуле $V_n = (2 \cdot E_y / m)^{0,5}$ и составляет $V_n$ = 112 м/с [1-3, 7, 9-10, 12, 15, 18, 19-20].

Рассмотрим дифференциальное уравнение (1) движения пули в воде на глубине 5 метров, гидростатическим давлением можно пренебречь. Произведем замену переменной $t$ на переменную $x$ в уравнении (2). После интегрирования получим формулу для убойного интервала пули $l_n$, позволяющую определить по формуле (3) неизвестное $k$ = 0,05.

Рассмотрим движение пули на глубине 20 м. Сила сопротивления воды: $F = \pi \cdot D^2/4 \cdot (P + k \cdot \rho_B \cdot V^2/2)$, здесь $P$ – статическая составляющая силы сопро-

тивления. Обозначим: $A = k \cdot \rho_B / 2$. Тогда: $F = \pi \cdot D^2 / 4 \cdot (A \cdot V^2 + P)$. Дифференциальное уравнение движения пули в воде на большой глубине имеет вид:

$$\frac{dV}{V^2 + C/A} = -\frac{\pi D^2 A}{4m} dt \tag{8.8}$$

$$\frac{2VdV}{V^2 + C/A} = -\frac{\pi D^2 A}{2m} dx \tag{8.9}$$

$$\int_{V_0}^{V_y} \frac{2VdV}{V^2 + C/A} = -\frac{\pi D^2 A}{2m} \int_0^{l_y} dx \tag{8.10}$$

$$\ln\left(V_y + C/A\right) - \ln\left(V_0^2 + C/A\right) = -\frac{\pi D^2 A}{2m} l_y \tag{8.11}$$

$$l_y = \frac{2m}{\pi A D^2} \ln \frac{V_0^2 + C/A}{V_Y^2 + C/A} \tag{8.12}$$

$$\ln_y = \frac{2m}{\pi A D^2} \ln \frac{AV_0^2 / C + 1}{AV_y^2 / C + 1} \tag{8.13}$$

Пусть $h = 20$ м, тогда $P = \rho \cdot g \cdot h = 2 \cdot 10^5$ Па, $l_П \approx 18$ м.

### *Результаты*

Результаты расчетов задач № 6, 7 приведены в таблице. В последней строке таблицы приводятся тактико-технические характеристики (ТТХ) автоматов. Расчетные данные согласуются с экспериментом.

*Таблица 1*

Согласование расчетных данных с характеристиками

| Характеристики пули | Автомат | |
|---|---|---|
| | АПС | АДС |
| Калибр $D$, мм | 5,66 | 5,45 |
| Масса $m$, г | 20 | 16 |
| Скорость $V_0$, м/с | 245 | 333 |
| Интервал $l_5$, м | 30 | 25 |
| Коэффициент $k$ | 0,04 | 0,05 |
| $l_{20}$, (расчет) | 19 | 20 |
| $l_{20}$, (ТТХ) | 18 | 18 |

## *Заключение*

Представлены инженерные модели проникания недеформируемых ударников в преграды: дерево, грунт, бетон, сталь, воду. Выполнены расчеты проникания типовых ударников, которые удовлетворительно согласуются с эмпирическими формулами. Перечисленные модели необходимы для решения военно-прикладных задач проникания боеприпасов в различные преграды.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Алексеевский В.П. К вопросу о проникании стержня в преграду с большой скоростью // Физика горения и взрыва. 1966. № 2.

2. Бабкин А.В. Средства поражения и боеприпасы: Учеб. / А.В. Бабкин, В.А. Велданов, Е.Ф. Грязнов и др.; Под общ. ред. В. В. Селиванова. – М.: Моск. гос. техн. ун-т, 2008.

3. Балаганский И.А., Мержиевский Л.А. Действие средств поражения и боеприпасов: Учебник. – Новосибирск Изд-во НГТУ. – 2004.

4. Брилев О. Танк на пороге XXI века (технический облик) // Военный парад. 1997. № 4 (22).

5. Водопьянов М.Я. Теория и расчет артиллерийских снарядов: Лабораторный практикум. – СПб.: БГТУ, 2002.

6. Воротилин М.С., Князева Л.Н., Чуков А.Н., Шмараков Л.Н. Современные средства поражения бронетанковой техники: учеб. пособие. Тула: ТулГУ, 2005.

7. Высокоскоростные ударные явления. – М.: Мир, 1973.

8. Григорян В.А., Белобородько А.Н., Терехин И.И. и др. Расчет и синтез структур баллистической защиты танков: Учеб. пособие / Под ред. В.А. Григоряна. – М.: МГТУ им. Н.Э. Баумана, 2006.

9. Григорян В.А., Белобородько А.Н., Дорохов Н.С. и др. Частные вопросы конечной баллистики / Под. ред. В.А. Григоряна. М.: МГТУ им. Н.Э. Баумана, 2006.

10. Зукас Дж. А., Николас Т., Свифт Х.Ф. и др. Динамика удара: Пер. с англ. М.: Мир, 1985.

11. Курков Б.А., Мураховский В.И., Сафонов Б.С. и др. Основные боевые танки / Под ред. Б.С. Сафонова и В.И. Мураховского. М.: Арсенал-Пресс, 1993.

12. Мержиевский Л.А., Титов В.М. Высокоскоростной удар // Физика горения и взрыва. 1987. № 5.

13. Носков Б.И. Малокалиберные выстрелы к автоматическим пушкам: учеб. пособие. М.: Изд-во «Вооружение. Политика. Конверсия», 1998.

14. Одинцов В. Танковое вооружение на пороге XXI века // Техника и вооружение. 1999. № 10.

15. Оружие и технологии России. Энциклопедия XXI век. Научно-техническое издание. Т. XII: Боеприпасы и средства поражения. М., 2006.

16. Прохоров Б.А. Боеприпасы артиллерии. М.: Машиностроение, 1973.

17. Растопшин М. Броня выигрывает соревнование. Концепция создания бронебойных подкалиберных снарядов нуждается в корректировке // Независимое военное обозрение. 2000. № 36.

18. Сагомонян А.Я. Проникание. М.: МГУ, 1974.

19. Физика быстропротекающих процессов. Т. 2 / Пер. с англ. Н.А. Златина. М.: Мир, 1971.

20. Фомин В.М., Гулидов А.И., Сапожников Г.А. и др. Высокоскоростное взаимодействие тел. Новосибирск: Изд. СО РАН, 1999.

УДК 234.465+534.222
DOI: 10.33764/2618-981X-2019-9-116-119

# ВЗРЫВОПОДОБНЫЕ ГЕОФИЗИЧЕСКИЕ ЯВЛЕНИЯ В АТМОСФЕРЕ ЗЕМЛИ

***Юрий Аркадьевич Николаев***
Институт гидродинамики им. М. А. Лаврентьева СО РАН, 630090, Россия, г. Новосибирск, пр. Академика Лаврентьева, 15

***Павел Аркадьевич Фомин***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат физико-математических наук, доцент кафедры специальных устройств, инноватики и метрологии; Институт гидродинамики им. М. А. Лаврентьева СО РАН, 630090, Россия, г. Новосибирск, пр. Академика Лаврентьева, 15, тел. (383)361-07-31, e-mail: kaf.suit@ssga.ru

Показано, что природа таких геофизических явлений, как озонный слой, озонные “дыры” и серебристые облака напрямую связаны с процессом самовоспламенения и цепного горения водорода в атмосфере, подобно тому, как это имеет место при взрыве облаков гремучей смеси. Это указывает на отсутствие прямой связи между деятельностью человека и образованием озонных “дыр”.

**Ключевые слова:** атмосфера земли, горение водорода, цепное воспламенение, взрыв, озонный слой, озонная “дыра”, серебристые облака.

# EXPLOSION-TYPE GEOPHYSICAS PHENOMENAS IN EARTH ATMOSPHERE

***Yuriy A. Nikolaev***
Lavrentiev Institute of Hydrodynamics SB RAS, 15, Prospect Akademik Lavrentiev St., Novosibirsk, 630090, Russia

***Pavel A. Fomin***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor of Department of Special Devices and Technologies; Lavrentiev Institute of Hydrodynamics SB RAS, 15, Prospect Akademik Lavrentiev St., Novosibirsk, 630090, Russia, phone: (383)361-07-31, e-mail: kaf.suit@ssga.ru

It was shown that the nature of such geophysical phenomena as the ozone layer, ozone “holes” and silvery clouds are directly related to the process of self-ignition and chain combustion of hydrogen in the atmosphere, similar to what occurs in the explosion of explosive clouds. This indicates the absence of a direct relationship between human activities and the formation of ozone “holes”.

**Key words:** Earth’s atmosphere, hydrogen combustion, chain ignition, explosion, ozone layer, ozone “hole”, noctilucent clouds.

В статье показано, что формирование озонного слоя, озонных “дыр” и серебристых облаков напрямую связано с процессом самовоспламенения и цепного горения водорода в атмосфере земли, подобно тому, как это имеет место при взрыве облаков гремучей смеси. Это указывает на отсутствие прямой связи

между деятельностью человека и образованием озонных “дыр”. При этом взрывную природу рассматриваемых явлений не следует буквально ассоциировать со взрывом или горением облака газовой смеси при нормальных условиях, поскольку рассматриваемые атмосферные процессы непрерывны, характеризуются огромными масштабами и происходят на больших высотах (и, соответственно, плотность сгораемого газа мала). Проведенное исследование основано на работе [1], при этом формула зависимости толщины озонного слоя от температуры и концентрации водорода у поверхности земли (см. ниже) является новой.

Исследован процесс горения водорода в атмосфере Земли. Аналитически решена одномерная система уравнений диффузии, теплопроводности и химической кинетики. Рассмотрены следующие реакции горения водорода: (1) $H + O_2 \rightarrow OH + O$; (2) $O + H_2 \rightarrow OH + H$; (3) $OH + H_2 \rightarrow H_2O + H$; (4) $H + O_2 + M \rightarrow HO_2 + M$. Реакция (1), как правило, при численном моделировании химических процессов в атмосфере, не рассматривается. На низких высотах ее влияние на процессы горения действительно пренебрежимо мало по сравнению с реакцией (4). Но, как установлено в работе, на высоте порядка 120 км расположен второй предел воспламенения, при котором скорости реакций (1) и (4) сравниваются. Выше скорость реакции (1) превышает скорость реакции (4), т.е. происходит цепное горение водорода. Реакции $O + O_2 + M \rightarrow O_3 + M$ и $O_3 + H_2 \rightarrow H_2O + O_2$ рассматриваются в качестве возникновения и гибели озона. Фотохимические процессы в атмосфере в рамках проведенного исследования не рассматривались. Общая схема химических процессов в атмосфере, связанная с цепным горением водорода, представлена на рисунке. Отметим, что излагаемый подход не является замкнутым, поскольку, например, распределение температуры в атмосфере по высоте не вычислялось, а полагалось известным.

Получено, что в результате цепной химической реакции водород практически полностью сгорает на высотах 120–200 км. Выше его концентрация вследствие цепного горения уменьшается с высотой с той же скоростью, что и давление, т.е. намного быстрее, чем это можно было ожидать из известной барометрической формулы. Таким образом, горение является причиной сохранения водорода атмосферой.

Реакция (1) является настолько мощным источником атомарного кислорода, что формирование озонного слоя Земли можно объяснить химическими реакциями, без учета фотодиссоциации кислорода. Получено, что суммарное содержание озона в атмосфере пропорционально концентрации водорода на поверхности Земли и зависит от ее температуры: $\Delta \sim [H_2]_0(1\text{-}T_0/400\ K)$, где $\Delta$ – эффективная толщина озонного слоя (толщина слоя, состоящего из молекул озона, который находится при нормальных условиях, и в котором собраны все молекулы озона, распределенные в атмосфере по высоте), $T_0$ – температура поверхности Земли. Рассматриваемая формула объясняет широтное распределение толщины озонного слоя на поверхности земного шара. Кроме того, из фор-

мулы следует, что существование озонных “дыр” можно объяснить неоднородным распределением водорода на поверхности Земли, а не антропогенным воздействием человека на окружающую среду (фреоны). Основной источник водорода в атмосфере – окисление углеводородов, автомобильные и индустриальные выбросы, сжигание биомассы. В свою очередь, рассматриваемые углеводороды формируются в природных влажных зонах (болота, пруды), рисовых чеках, вследствие биоферментации, промышленных выбросов и сгорания топлив. В то же время, практически нет источников водорода в Антарктиде, зонах обледенения и областях вечной мерзлоты зимой. Это и является причиной образования озонных “дыр” в таких областях. Озонный слой “дышит”: озонные “дыры”, например, могут образовываться весной и летом и исчезать зимой.

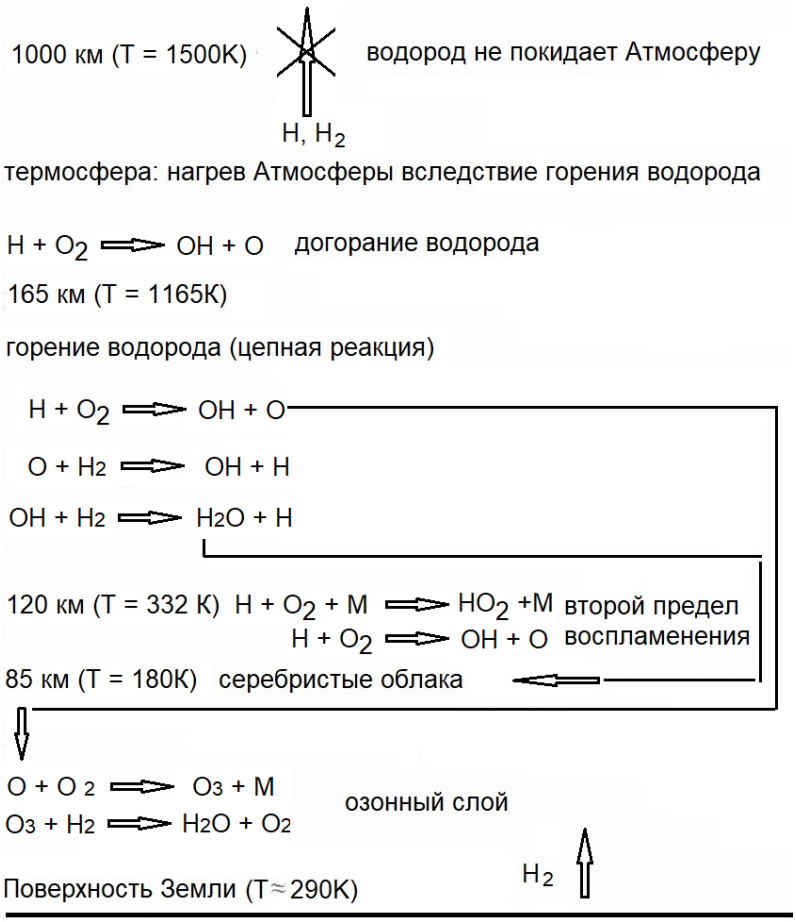



Схема процесса горения в атмосфере Земли

Одним из продуктов горения водорода в верхних слоях атмосферы являются пары воды, которые диффундируют вниз. На высотах порядка 85 км при флуктуационном понижении температуры образуются льдинки, количества которых достаточно для образования в сумерках серебристых облаков.

Как следует из проведенного исследования, озонные “дыры” не связаны с активностью человека. Поэтому к международным договорам, накладываю-

щим дорогостоящие ограничения на промышленное производство с целью “восстановления” озонного слоя (например, ограничение производства фреоносодержащих веществ) и, соответственно, влияющие на благосостояние развивающихся стран, необходимо относиться более критично.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ю.А. Николаев, П.А. Фомин. О природе серебристых облаков и озонного слоя Земли. Физика горения и взрыва, 1997, 33, 4, с. 3-13.

УДК 621.373.8
DOI: 10.33764/2618-981X-2019-9-120-125

# ЛАЗЕРНОЕ ЗОНДИРОВАНИЕ ВЗРЫВЧАТЫХ ВЕЩЕСТВ МЕТОДОМ ДИФФЕРЕНЦИАЛЬНОГО ПОГЛОЩЕНИЯ И РАССЕЯНИЯ

***Валерик Сергеевич Айрапетян***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, зав. кафедрой специальных устройств инноватики и метрологии, тел. (383)361-07-31, e-mail: v.s.ayrapetyan@sgga.ru

***Александр Викторович Макеев***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, аспирант, e-mail: makeeffsan@yandex.ru

Предложена схема лидарного комплекса для дистанционной идентификации взрывчатых веществ методом дифференциального поглощения и рассеяния. Проведены расчетные исследования по дистанционному исследованию спектроскопических параметров некоторых взрывчатых веществ (TNT, TATR, DNT).

**Ключевые слова:** лидар, перестраиваемый генератор света, метод дифференциального поглощения и рассеяния, нелинейный кристалл, HGS, взрывчатое вещество.

# EXPLOSIVES LASER PROBING BY DIFFERENTIAL ABSORPTION AND SCATTERING

***Valerik S. Ayrapetyan***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Head of Department of Special Devices for Innovation and Metrology, phone: (383)361-07-31, e-mail: v.s.ayrapetyan@sgga.ru

***Alexander V. Makeev***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D. Student, e-mail: makeeffsan@yandex.ru

A scheme of a lidar complex for remote identification of explosives by the method of differential absorption and scattering is proposed. Computational studies on the remote study of the spectroscopic parameters of some explosives (TNT, TATR, DNT) were carried out.

**Key words:** lidar, tunable light generator, differential absorption and scattering method, nonlinear crystal, HGS, explosive.

## *Введение*

В современном мире наблюдается тенденция к росту терроризма. Так военная доктрина Российской Федерации в пункте 12 (к) относит растущую угрозу глобального экстремизма (терроризма) и его новых проявлений в условиях недостаточно эффективного международного антитеррористического сотрудничества, реальную угрозу проведения терактов с применением радиоактивных и токсичных химических веществ, к основным внешним военным опасностям,

угрожающим нашей стране. Оптические методы обнаружения взрывчатых веществ с использованием лазерного излучения в диапазоне 1,41 – 9,0 мкм обладают рядом преимуществ перед широко распространенными контактными методами обнаружения взрывчатых веществ. Поэтому задача создания новых высокоэффективных комплексов дистанционного обнаружения и идентификации взрывчатых веществ, основанных на методах лазерной ИК-спектроскопии для оснащения специальных служб РФ является крайне актуальной, для обеспечения безопасности и обороноспособности страны.

В связи с актуальностью рассматриваемой проблемы активно ведутся работы по совершенствованию и разработке новых методов обнаружения взрывчатых веществ.

Среди аппаратных средств поиска взрывоопасных устройств по прямым признакам (наличию взрывчатых веществ и отдельных его компонентов) распространены газоаналитические приборы. Достаточно полный обзор промышленно выпускаемых отечественных и импортных газоанализаторов представлен в работе [1]. Ряд работ посвящен дистанционному обнаружению взрывчатых веществ с помощью излучения оптического диапазона. Обнаружение и идентификация взрывчатого вещества в таких работах производится с использованием различных методов спектроскопии. Так в работе [2] приведены результаты полевых испытаний установки, работающей по методу спектроскопии комбинационного рассеяния, поверхностная концентрация обнаруженных следов взрывчатых веществ (аммоний нитрат и тринитротолуол) на расстоянии 10 м составила до 10 пг/см$^2$. С применением аналогичного метода авторам работы [3] удалось обнаружить следы гексогена и пентаэритриттетранитрата массой менее 1 мг и следы тринитротолуола массой 700 мкг на расстоянии 20 м. Результаты применения спектроскопии когерентного актистоксова комбинационного рассеяния света для дистанционного обнаружения следов $KNO_3$ и гексогена на расстояниях до 12 м было продемонстрировано в работе [4]. Лазерно-индуцированная флуоресценция продуктов фотофрагментации взрывчатых веществ представлена в работах [5,6] пороговая чувствительность данного метода составляет около десятков-сотен ppt на дистанции более 10 метров. Метод лазерной фототермической спектроскопии применен в работе зарубежных ученых, результатом стало определение следов тринитротолуола на расстоянии 150 метров [7]. В работе [8] использован метод активного формирования спектральных изображений среднее значение обнаружения взрывчатого вещества при использовании данного метода составило 0,84мг/см$^2$, дистанция обнаружения 0,4 метра, также данный метод применен в работах зарубежных ученых[9–12].

## *Методы и материалы*

В данной работе предложен метод обнаружения и идентификации взрывчатых веществ на основе лидарного комплекса, использующего в качестве источника излучения инфракрасный параметрический генератор света (ИК-ПГС).

Рассматриваемый метод основан на том, что в средней ИК области, от 2500 $см^{-1}$ (4 мкм) до 1100 $см^{-1}$ (9 мкм), колебательно-вращательные спектры поглощения молекул взрывчатых веществ обладают высокой специфичностью, определяемой их симметрией и химическим составом, что позволяет с достаточной точностью относить отдельные спектральные линии к вполне определенному химическому соединению. Именно в этой области спектра находятся фундаментальные колебательно-вращательные переходы молекул практически всех известных взрывчатых веществ.

На рис. 1 представлена схема лидарного комплекса для дистанционного обнаружения взрывчатых веществ.

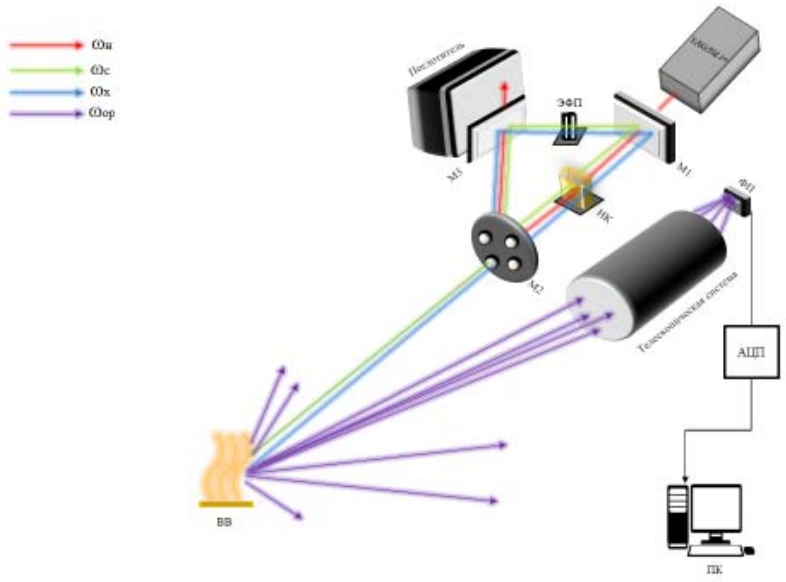



Рис. 1. Схема ИК-параметрического лидарного комплекса

Источником накачки служит импульсный YAG: $Nd^{3+}$ – лазер, плавная перестройка частоты $\omega_c$, $\omega_x$ осуществляется посредством поворота нелинейного кристалла (НК) из HGS, сам резонатор выполнен по кольцевой схеме и состоит из зеркал М1, М2, М3, причем зеркало М2 выполнено в виде набора зеркал, размещенных на револьверном механизме, для оптимизации коэффициента отражения, а зеркало М3 имеет пропускание на частоте $\omega_н$ излучения накачки, которое попадает в специально установленный поглотитель, обеспечивая тем самым оптимальный режим работы диспергирующего элемента в виде эталона Фабри-Перо (ЭФП), АЦП – аналогово-цифровой преобразователь; ПК – персональный компьютер

Сам метод поиска и обнаружения взрывчатого вещества (ВВ) основан на принципе дифференциального поглощения и рассеяния (ДПР). С помощью установки, посредством плавной перестройки частоты излучения, лазерный импульс, проходя через взрывчатое вещество, устанавливается на максимуме линии поглощения в т. В, затем, на крыле этой линии в т. А (рис. 2).

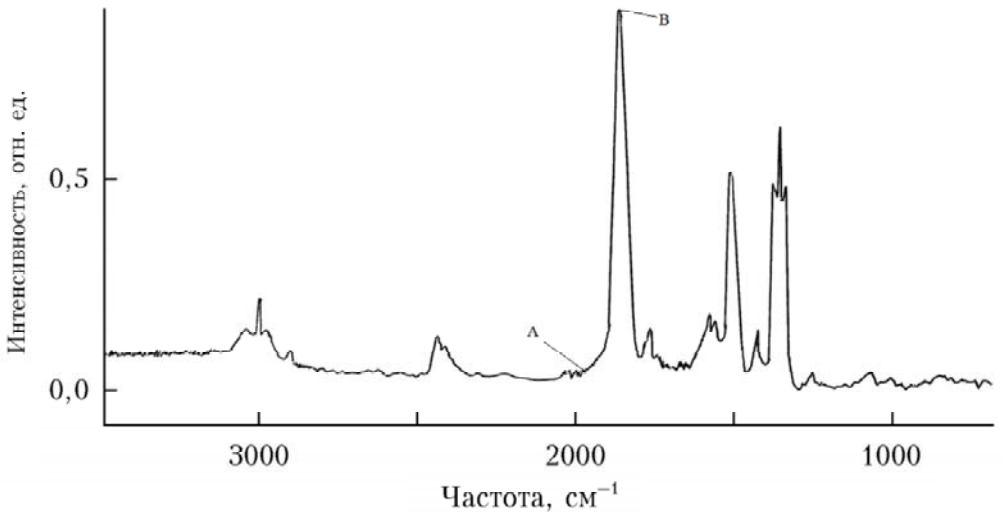



Рис. 2. ИК-Фурье спектр поглощения ТЭН (пентаэритриттетранитрат) в инфракрасном диапазоне частот от 3500 до 500 см$^{-1}$ [13]

Сигналы двух импульсов регистрируются фотодетектором и сравниваются в АЦП. Дифференциальное значение этих двух сигналов выводится на монитор ПК в виде колебательно-вращательных спектров поглощения молекулами ВВ. Метод ДПР обладает наилучшей чувствительностью при зондировании определенных составляющих с больших расстояний [14–16].

Расчет полуширины лазерного излучения выполнен по формуле:

$$\Delta\vartheta = \frac{\lambda_2 - \lambda_1}{\lambda_0^2}. \quad (1)$$

На основе интенсивностей были вычислены объемные коэффициенты обратного рассеяния $\beta(\lambda_0, R)$ на длине волны $\lambda_0$ и расстоянии до объекта R, а затем получено значение минимальной выходной энергии зондирующего лазера для детектирования минимальной концентрации ВВ в соответствии с формулой

$$E_{Lmin} \approx \frac{2R^2 \cdot (\frac{С}{Ш})_{min}}{\beta(\lambda_0 R) \cdot \xi(\lambda_0) \cdot U(\lambda_0)} \exp\left[2\int_0^R k(\lambda_0 R)dR\right], \quad (2)$$

где С/Ш – отношение интенсивности сигнала к шуму;

$\xi(\lambda 0)$ – коэффициент спектрального пропускания приемной оптической системы;

$U(\lambda 0)$ – параметр чувствительности приемной системы;

$k(\lambda 0, R)$ – коэффициент ослабления на соответствующей длине волны $\lambda 0$.

Учитывая, что отношение интенсивности сигнала к шуму для данной системы равно 1,5, зная величины параметров лазерной установки ($\xi(\lambda 0) = U(\lambda 0) = 1$), с учетом проведения экспериментальных исследований в лабораторных условиях ($R$ = 5 см) по формуле (1) получим, что минимально необходимая энергия зондирующего лазера будет равна 10 мДж.

По значениям минимальной выходной энергии зондирующего сигнала, объемного коэффициента обратного рассеяния и расстояния до объекта вычислена интенсивность прошедшего сигнала (E) через молекулы вещества, TNT, TATR, DNT по формуле Бэра:

$$E = E_{Lmin} \cdot e^{-\beta R}. \quad (3)$$

Величина концентрации органических веществ N(R) в объеме газа, определяемая методом ДПР рассчитана по формуле:

$$N(R) = \frac{1}{2\sigma_A(\lambda_0-\lambda_1)}\left\{\frac{d}{dR}\left[ln\frac{P(\lambda_1,R)}{P(\lambda_0,R)} - ln\frac{\beta(\lambda_1,R)}{\beta(\lambda_0,R)}\right] + k(\lambda_1,R) - k(\lambda_0,R)\right\}. \quad (4)$$

## *Результаты*

Расчеты спектроскопических параметров для веществ TNT, TATR, DNT представлены в таблице.

Результаты расчета спектроскопических параметров ВВ

| Наименование вещества | Максимальная частота поглощения, ν, $см^{-1}$ | Длина волны, λ, мкм | Полуширина излучения, Δν, $см^{-1}$ | Коэффициент поглощения, α, $см^{-1}$ | Концентрация веществ, ppm |
|---|---|---|---|---|---|
| TNT | 1850±0,7 | 5,405 | 56,1±1 | $1{,}78\cdot10^{-11}$ | 10 |
| DNT | 1349±0,7 | 7,41 | 36,5±1 | $1{,}8\cdot10^{-10}$ | 11 |
| ТАТР | 1373±0,6 | 7,28 | 37,7±1 | $1{,}1\cdot10^{-10}$ | 20 |

## *Заключение*

Таким образом в работе проведен анализ современного состояния средств обнаружения и идентификации ВВ, предложена схема ИК-параметрического лидарного комплекса для обнаружения и идентификации ВВ методом ДПР, представлены расчетные спектроскопичекие параметры для ВВ типа TNT, TATR, DNT.

## *Благодарности*

Работа выполнена при поддержке РФФИ (грант №19-45-700003).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кихтенко А.В., Елисеев К.В. Обнаружение взрывоопасных объектов: аппаратурное обеспечение антитеррористических служб // Ж. Рос. хим. об-ва им. Д.И. Менделеева. – 2005, Т. XLIX №4 – 132-137 С.

2. E.Ceco, H. Önnerud, D. Menning, J.L. Gilljam, P. Baath, H. Östmark, Stand-off imaging Raman spectroscopy for forensic analysis of post-blast scenes – Trace detection of ammonium ni-

trate and 2,4,6-trinitrotoluene. – Chemical, Biological, Radiological, Nuclear, and Explosives Sensing XV, Proc. of SPIE, Vol. 9073, 90730G. – 2014. – pp. 1-9.

3. Zachhuber B., Ramer G., Horbo A., Lendl B., Stand-off Raman specroscopy of explosives, Proc. of SPIE, Vol. 7838, 78380F (2010), p. 1-10.

4. Katz O., Natan A., Silberberg Y., Rosenwaks S. Standoff detection of trace amounts of solids by nonlinear Raman spectroscopy using shaped femtosecond pulses // Appl. Phys. Lett. 2008. V. 92, N 17. P. 171116.

5. Wynn C. M.; Palmacci S.; Kunz R. R.; Rothschild M. A Novel Method for Remotely Detecting Trace Explosives. – Lincoln Laboratory Journal, 17, №2, (2008), pp. 27–39.

6. Wynn C.M., Palmacci S., Kunz R.R., Aernecke M. Noncontact optical detection of explosive particles via photodissociation followed by laser-induced fluorescence // Opt. Express. 2011. V. 19, N 19. P. 18671–18677.

7. Mukherjee A., Porten S., Patel C.K.N. Standoff detection of explosive substances at distances of up to 150 m // Appl. Opt. 2010. V. 49. N 11. P. 2072–2078.

8. Кузовникова Л.В. Определение характеристик оптико-электронного комплекса обнаружения следов ВВ. / Л.В. Кузовникова, Е.В. Максименко // Южно-Сибирский научный вестник. – 2017. – № 3. – С. 74–77.

9. Morales-Rodrígueza M. E., SenesacaL.Thundat T., Rafailov M. K., Datskos P. G. Standoff imaging of chemicals using IR spectroscopy. – Proc. of SPIE, Vol. 8031, 80312D (2010), pp. 1–8.

10. Ruxton K., Robertson G., Miller W., Malcolm G.P.A., Maker G.T. Mid-infrared hyperspectral imaging for the detection of explosive compounds. – Proc. of SPIE Vol. 8546, 85460V (2012), pp. 1-9.

11. Bernacki B. E., Blake T.A., Mendoza A., Johnson T.J. Visible hyperspectral imaging for standoff detection of explosives on surfaces. – Proc. of SPIE Vol. 7838, 78380C (2010), pp. 1-7.

12. Hempler N., Nicholls J., Malcolm G. Active hyperspectral sensing and imaging for remote spectroscopy applications (2013) http://www.laserfocusworld.com/articles/print/volume-49/issue-11/features/spectral-imaging-active-hyperspectral-sensing-and-imaging-for-remote-spectroscopy-applications.html.

13. Спектрохимические особенности некоторых бризантных взрывчатых веществ в парообразном состоянии / Набиев Ш.Ш., Ставровский Д.Б., Палкина Л.А., Збарский В.Л., Юдин Н.В., Голубева Е.Н., Вакс В.Л, Домрачева Е.Г., Собакинская Е.А., Черняева М.Б. // Оптика атмосферы и океана, 2013, 26 №4 – С. 273-285.

14. Айрапетян В. С., Маганакова Т. В. Обнаружение и измерение параметров наркотических веществ с помощью перестраиваемого ИК-лазера // Интерэкспо ГЕО-Сибирь-2014. X Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2014» : сб. материалов в 2 т. (Новосибирск, 8–18 апреля 2014 г.). – Новосибирск : СГГА, 2014. Т. 2. – С. 199–204.

15. Айрапетян В. С., Маганакова Т. В. Лазерное зондирование в задаче обнаруженияи измерения параметров наркотических веществ // Вестник СГГА. – 2014. – Вып. 2 (26). – С. 40–46.

16. Айрапетян В. С., Маганакова Т. В. Расчет концентрации наркотических веществметодом дифференциального поглощении и рассеяния // Интерэкспо ГЕО-Сибирь-2015. XI Междунар. науч. конгр. : Междунар. науч. конф. «СибОптика-2015» : сб. материалов в 3 т. (Новосибирск, 13–25 апреля 2015 г.). – Новосибирск : СГУГиТ, 2015. Т. 1. – С. 141–147.

УДК 621.372.413
DOI: 10.33764/2618-981X-2019-9-126-130

# ЭЛЕКТРОДИНАМИЧЕСКОЕ ПРОЕКТИРОВАНИЕ ЭЛЕМЕНТОВ СВЯЗИ ПОЛОСОВЫХ ФИЛЬТРОВ

***Константин Якубович Аубакиров***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного 10, кандидат технических наук, доцент кафедры специальных устройств, инноватики и метрологии, тел. (383)361-07-31

***Александр Викторович Макеев***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного 10, аспирант, тел. (383)361-07-31, e-mail: makeeffsan@yandex.ru

***Анна Евгеньевна Жукова***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (383)361-07-31

В работе предложена методика проектирования элементов связи между резонаторами полосового фильтра.

**Ключевые слова:** электрические фильтры, электромагнитная совместимость, настройка.

# ELECTRODYNAMIC DESIGN OF STRIP FILTER COMMUNICATIONS

***Konstantin Ya. Aubakirov***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor of Department of Special Devices for Innovation and Metrology, phone: (383)361-07-31

***Alexander V. Makeev***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D. Student, e-mail: makeeffsan@yandex.ru

***Anna E. Zhukova***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (383)361-07-31

A method for designing communication elements between resonators of a bandpass filter is offered.

**Key words:** electrical filters, electromagnetic compatibility, configuration.

## *Введение*

Как показано в [1], методика проектирования электрических фильтров по рабочим параметрам, основанная на использовании низкочастотных фильтров-

прототипов, позволяет определить как внешние добротности первого и последнего резонатора фильтра:

$$(Q_e)_A = \frac{g_0 g_1 \omega_1'}{w} = \frac{b_1}{\left(J_{01}^2 / G_A\right)}, \quad (Q_e)_B = \frac{g_n g_{n+1} \omega_1'}{w} = \frac{b_n}{\left(J_{n,n+1}^2 / G_B\right)},$$

так и коэффициенты связи между $j$ и $j+1$ резонаторами

$$k_{j,j+1|j=1\div n-1} = \frac{w}{\omega_1' \sqrt{g_j g_{j+1}}},$$

где $g_0 \div g_{n+1}$ – параметры нормированного фильтра прототипа [3], $b_1 \div b_n$ – параметры крутизны резонаторов фильтра [2, т.1], $\omega_0 = \frac{\omega_2 + \omega_1}{2}$ и $w = \frac{\omega_2 - \omega_1}{\omega_0}$ – центральная частота полосы пропускания фильтра и соответственно относительная полоса пропускания, $J_{01}$ и $J_{n,n+1}$ – параметры инверторов проводимости, обеспечивающих внешние добротности идеального сосредоточенного фильтра, нагруженного на проводимости $G_A$ и $G_B$.

Предложенная в [1] методика расчета настроечных кривых по методу Dishal [5], используя [4], показала высокую эффективность при настройке 6-ти и 8-ми резонаторных фильтров для систем цифрового телевидения.

В то же время определение геометрических размеров элементов связи между одинаковыми объемными резонаторами [2] требует решения электродинамической задачи для окон в стенках конечной толщины. Такая возможность реализуется в рамках 3D моделирования с помощью «GST Studio Suite» для пары резонаторов [2, т.2].

Так как в диапазоне дециметровых телевизионных каналов расчетная величина $k_{j,j+1}$ лежит в интервале от 0,0092 до 0,017, использование этой методики [4] представляется целесообразным как для определения резонансной частоты и собственной добротности резонаторов (рис. 1), так и для проектирования регулируемых элементов связи между резонаторами с заданными пределами изменения $k_{j,j+1}$ (рис. 3, *а*, *б*).

### *Результаты*

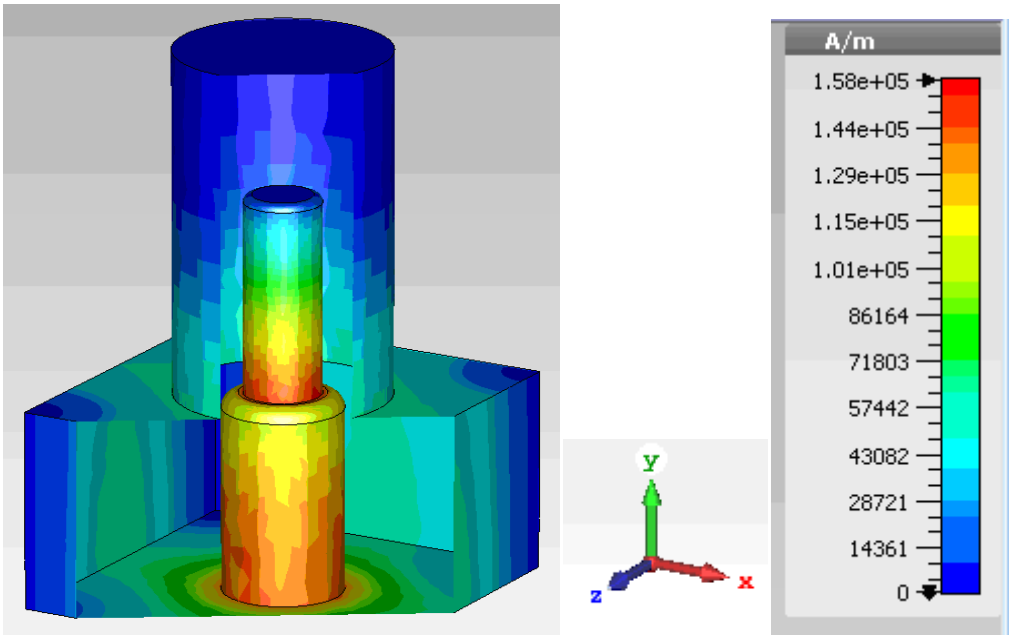
Сборка из двух резонаторов (рис. 1) представлена на (рис. 2), а в табл. 1 приведены результаты расчета коэффициента связи в зависимости от ширины «окна».

*Таблица 1*

Зависимость коэффициента связи пары резонаторов от ширины окна – $S$

| $S$ [мм] | 10 | 20 | 24 | 28 | 32 |
|---|---|---|---|---|---|
| $k_{j,j+1}$ | $1,25\cdot10^{-3}$ | $1,76\cdot10^{-3}$ | $3,057\cdot10^{-3}$ | $4,562\cdot10^{-3}$ | $5,982\cdot10^{-3}$ |

Зависимость $k_{j,j+1}$ от $S$ для «сборки» (рис.2) была определена для полосковой части резонатора прямоугольного сечением $b=85\times85$ мм и диаметре внутреннего короткозамкнутого проводника равном $d=28$ мм, высота области связи $h=78$ мм. Коаксиальная часть резонатора характеризуется: $D=27,5$ и $d=9$ мм, изменением длины этой части, обеспечивается грубая перестройка в диапазоне частот.




*а*) *б*)

Рис. 1. Электромагнитная модель резонатора смешанной коаксиально-полосковой конструкции для определения резонансной частоты:

*а*) распределение плотности тока проводимости; *б*) шкала напряженности магнитного поля на поверхности проводника

Предложенный в [2 т.2] метод определения коэффициента связи между двумя одинаковыми резонаторами, требует получения двугорбой кривой коэффициента передачи (связь выше критической) и, как следствие, установку двух Waveguide Port и сопутствующих им дополнительных элементов связи. Также анализ кривых $\left|S_{21}(\omega)\right|^2$ требует дополнительных затрат времени.

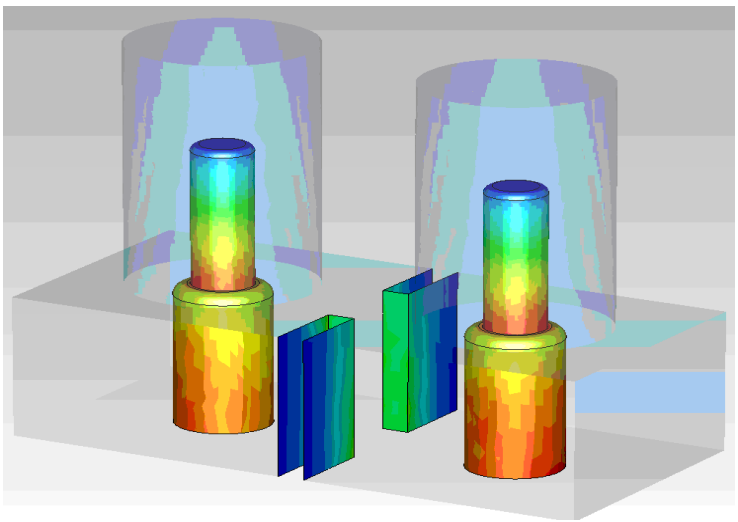
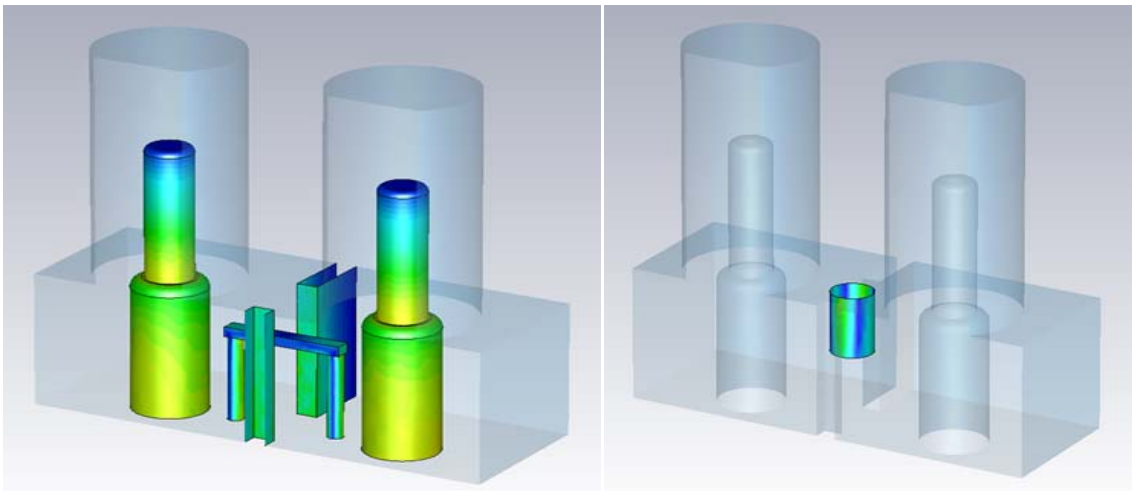


Рис. 2. Сборка двух резонаторов, связанных через «окно» в перегородке



*а*) *б*)

Рис. 3. Два резонатора, связанных регулируемыми элементами связи:
*а*) связанных короткозамкнутой петлей; *б*) связанных короткозамкнутым винтом в «окне»

## *Заключение*

В настоящей работе использован альтернативный способ вычисления коэффициента связи. Так, при задании в плоскости симметрии, разделяющей связанные по электромагнитному полю объемы, электрической и магнитной стенки, в режиме Eigenmode Calculation определяются две частоты – $f_{H_{\tau=0}}$ и $f_{E_{\tau=0}}$ с высокой точностью. Тогда $k_{\text{св}} = \dfrac{\left| f_{H_{\tau=0}} - f_{E_{\tau=0}} \right|}{\sqrt{f_{H_{\tau=0}} \cdot f_{E_{\tau=0}}}}$ для соответствующей

пары резонаторов. Данные табл. 1 позволяют определить минимально необходимый коэффициент связи из соображений электрической прочности фильтра. Увеличение последнего при настройке осуществляется перемещением короткозамкнутых винта и петли (рис. 3, *а*, *б*).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Полоснопропускающие фильтры из цепочек одинаковых резонаторов для решения задач электромагнитной совместимости / К. Я. Аубакиров, А. Г. Вихорев, В. П. Разинкин, А. В. Макеев // Интерэкспо ГЕО-Сибирь-2016. XII Междунар. науч. конгр. : Междунар. науч. конф. «Специальные вопросы фотоники: Наука. Оборона. Безопасность» : сб. материалов (Новосибирск, 18–22 апреля 2016 г.). – Новосибирск : СГУГиТ, 2016. – С. 42–48.

2. Маттей Д. Л., Янг Л., Джонс Е. М. Т. Фильтры СВЧ, согласующие цепи и цепи связи. В 2 томах: Пер. с англ. / Л. В. Алексеева и Ф. В. Кушнира. – М.: Связь, т. 1 1971. – 440 с., т. 2 1972. – 496 с.

3. Ханзел Г. Е. Справочник по расчету фильтров. – М.: Советское радио, 1974. – 288 с.

4. Курушин А. А. Школа проектирования СВЧ – устройств в GST Studio Suite / А. А. Курушин.- М.: Сам полиграфист, 2014. – 433 с.

5. Разевиг В.Д. Проектирование СВЧ устройств с помощью Microwave Office / В.Д. Разевиг, Ю.В. Потапов, А.А. Курушин. – М.: СОЛОН-Пресс, 2003.- 496 с.

6. Dishal M. Alignment and Adjustment of Synchronously Tuned Multiple-Resonant-Circuit Filters.-«Proc. IRE», Nov. 1951, v. 39, № 11, pp. 1448-1455.

УДК 520.0.03
DOI: 10.33764/2618-981X-2019-9-131-136

# МОДУЛЬНЫЕ КОМПЛЕКСЫ НА БАЗЕ ЛАЗЕРНЫХ ДАЛЬНОМЕРОВ

***Николай Николаевич Бардачевский***
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат географических наук, доцент кафедры специальных устройств, инноватики и метрологии, тел. (383)361-07-31, e-mail: bardachevskiy@ngs.ru; Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, доцент кафедры, тел. (383)332-50-45

***Владимир Анатольевич Литовченко***
Новосибирское высшее военное командное училище, 630117, Россия, г. Новосибирск, ул. Иванова, 49, начальник инструкторской группы кафедры разведки (и воздушно-десантной подготовки), тел. (383)332-50-45, e-mail: litovchienko.vladimir@mail.ru; Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, аспирант, тел. (923)100-89-86

В статье рассматриваются основные тенденции совершенствования современных оптико-электронных средств наблюдения, созданных на базе лазерных дальномеров.

**Ключевые слова:** лазерный дальномер, прибор ночного видения, тепловизионный прибор, оптико-электронное средство наблюдения, модуль оптико-электронный, координаты, электронный тахеометр.

# MODULAR COMPLEXES ON THE BASIS OF LASER RANGE

***Nikolai N. Bardachevsky***
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, of Special Devices for Innovation and Metrology, phone: (383)361-07-31, e-mail: bardachevskiy@ngs.ru; Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Associate Professor, phone: (383)332-50-45

***Vladimir A. Litovchenko***
Novosibirsk Higher Military Command School, 49, Ivanova St., Novosibirsk, 630117, Russia, Head of Instructor Group, Department of Educational Intelligence (and Airborne Training), phone: (383)332-50-45, e-mail: litovchienko.vladimir@mail.ru; Siberian State University of Geosystems and Technologies, 10 , Plakhotny St., Novosibirsk, 630108, Russia, phone: (923)100-89-86

The article discusses the main trends in the improvement of modern optoelectronic surveillance tools created on the basis of laser rangefinders.

**Key words:** laser range finder, night vision device, thermal imaging device, optoelectronic surveillance tool, optoelectronic module, coordinates, electronic total station.

## *Введение*

Развитие лазерных дальномеров военного и гражданского назначений связано с совершенствованием их основных тактико-технических характеристик.

Естественно, что для каждого применения дальномера устанавливаются свои требования к тем или иным характеристикам. Приоритетными направлениями развития являются повышение точности измерений и дальности действия, улучшение массогабаритных характеристик. В последнее время наблюдается тенденция к переходу на излучатели, позволяющие осуществлять генерацию на безопасной для зрения длине волны. Для увеличения функциональных возможностей лазерные дальномеры оснащаются специальными устройствами, обеспечивающими выполнение той или иной функции.

Одной из серьезных задач, решенных при создании оптико-электронных средств, было создание многоканальных комплексов, а также приборов, которые должны обеспечивать решение задачи непрерывного наблюдения за местностью, разведки цели и прицеливания как в дневное, так и в ночное время [3].

## *Методы и материалы*

Современные лазерные дальномеры способны выполнять не только свою первостепенную функцию – измерение дальности, но и дополнительные функции, для обеспечения выполнения которых дальномеры оснащаются специальными средствами. Это могут быть угломерные устройства, электронный компас, GPS приемники и др. Кроме того, возможны варианты объединения лазерных дальномеров, например, с тепловизионными устройствами или приборами ночного видения (ПНВ).

Для современных лазерных дальномеров требуется обеспечение круглосуточной работы, что приводит к необходимости объединения лазерного дальномера с ПНВ. Если ПНВ имеет переносное исполнение (то есть с возможностью установки на треноге), то для создания прибора круглосуточного действия достаточно предусмотреть посадочную поверхность на корпусе ПНВ для закрепления на ней лазерного дальномера. При этом на корпусе лазерного дальномера должна быть смонтирована ответная часть такого крепления с фиксатором.

Если же ПНВ представляет собой удерживаемое в руках (ночной бинокль) либо наголовное устройство (очки ночного видения), то используют другие способы объединения. В частности, возможно объединение лазерного дальномера с ПНВ в результате согласования окулярной части визира лазерного дальномера с микроскопом ночного бинокля. При этом лазерный дальномер должен располагаться сбоку по отношению к корпусу ночного бинокля, а его окулярная система должна быть оптически сопряжена с ветвью псевдобинокулярного микроскопа ночного бинокля [5].

Благодаря созданию полупроводниковых многоэлементных фотоприемных устройств для работы в области спектра от 1 до 1,7 мкм, применяемых в ПНВ, появляется возможность работы ПНВ совместно с лазерными дальномерами, работающими на длине волны от 1,54 до 1,55 мкм. В таких биноклях используются два канала, которые работают в диапазонах от 0,4 до 0,9 мкм и от 1 до 1,7 мкм, а также лазерный дальномер, действующий в диапазоне от 1,54 до 1,55 мкм [7].

Для определения координат как самого наблюдателя, так и цели в некоторых моделях современных дальномеров размещают спутниковые навигационные приемники.

Многие современные лазерные дальномеры оснащаются угломерными устройствами, это позволяет измерять магнитные азимуты, горизонтальные и вертикальные углы. Оснащение лазерного дальномера цифровым магнитным компасом позволяет не только ориентироваться по сторонам света, но и измерять углы по вертикали и горизонтали с точностью до 0,1º [15].

Как уже было упомянуто выше, на базе совместного использования электронных дальномеров и электронных теодолитов создаются комбинированные приборы, которые получили название электронных тахеометров, применяемых в основном в геодезии. Электронные тахеометры позволяют в автоматизированном режиме выполнять измерения как длин линий, так и углов, а также вычислять величину взаимного превышения концов искомой линии, горизонтальное положение, погрешность выполненных измерений и другие интересующие потребителей величины [2]. Стоит сказать, что объединение дальномеров с угломерными устройствами и разработка тахеометров является одним из основных направлений развития фазовых дальномеров [1].

Таким образом, благодаря осуществлению подобных объединений и оснащению лазерных дальномеров различными устройствами, увеличиваются функциональные возможности первых и, как следствие, расширяется область их применения.

В настоящее время в состав прицельно-наблюдательных комплексов образцов вооружения и военной техники сухопутных войск традиционно входят оптико-электронные каналы разведки, наблюдения и прицеливания видимого, ближнего и дальнего ИК-диапазонов [10].

При использовании противником качественной маскировки обнаружение и распознавание объекта затруднено, соответственно вероятность обнаружения и распознавания замаскированного объекта на типовых тактических дальностях может быть близка к нулю [4].

Действительно, тепловизионная техника, обеспечивающая наблюдение в условиях плохой видимости днем и ночью, является в настоящее время единственным средством, способным повысить эффективность боевых действий при решении тактических задач, так как возможности ПНВ всех поколений в значительной степени определяются уровнем освещенности и прозрачностью атмосферы [18].

Тепловизионные приборы свободны от этих недостатков, поэтому их использование в качестве прицелов к тактическому оружию, по мнению зарубежных специалистов, является предпочтительным, тем более что они обеспечивают решение боевой задачи в течение суток, а не только ночью, как ПНВ [17].

В последнее время хорошо зарекомендовали себя на практике и совершенствуются многоканальные комплексы, объединяющие в себе лазерные дальномеры и тепловизионные приборы, используемые в военном деле.

Как правило, в состав таких многоканальных комплексов входят:

- оптико-электронный модуль;
- механизм наведения;
- тренога.

Основной частью таких приборов является оптико-электронный модуль. Применение приборов по назначению возможно «с рук», без установки оптико-электронного модуля на механизм наведения и треногу. Для повышения точности наведения и определения координат при работе по малоразмерным целям на больших дальностях – с использованием треноги с механизмом наведения. Кроме того предусмотрена возможность установки оптико-электронного модуля через кронштейн на буссоль или углоизмерительное устройство лазерного дальномера ЛПР-1 [9].

Для обеспечения наблюдения, поиска и распознавания целей оптико-электронный модуль включает в себя телевизионный канал, работающий в видимом диапазоне, и тепловизионный канал, работающий в инфракрасном диапазоне, обеспечивающие работу прибора в любое время суток.

Для ориентации на местности и измерения координат разведанных объектов в оптико-электронный модуль прибора входят:

- электронный компас, обеспечивающий измерение горизонтальных углов, а также углов места и крена;
- устройство радионавигационное, которое обеспечивает прием и обработку навигационных сигналов, передаваемых спутниками системы глобального позиционирования Global Position System (GPS) или глобальной навигационной спутниковой системы (ГЛОНАСС) и определение в реальном времени координат местоположения прибора в системах координат Гаусса-Крюгера (Г-К), ПЗ-90, WGS-84, СК-42, СК-95.

## *Результаты*

Приборы данной серии обеспечивают автоматическое преобразование измеренных сферических координат цели и координат «точки стояния» прибора в прямоульные или геодезические координаты цели и отображают их на видеосмотровом устройстве [8].

Измерение дальности обеспечивается лазерным дальномерным каналом, диапазон измерения которого, в зависимости от модификации прибора, достигает 4000–7000 м [12].

Измеренные и вычисленные значения координат целей и их видеоизображения могут записываться и храниться в запоминающем устройстве прибора.

Текущее изображение наблюдаемой «сцены» с выхода телевизионного или тепловизионного канала, значения измеренных координат и служебная информация отображаются на двух микродисплеях видеосмотрового устройства (отдельных для каждого глаза).

Оба наблюдательных канала, обеспечивают возможность электронного увеличения изображения $2^{\times}$ и $4^{\times}$.

Также в приборах обеспечивается возможность просмотра записанных в запоминающее устройство прибора координат целей и видеокадров с изображением этих целей на видеосмотровое устройство и вывода их на внешние устройства других сопрягающихся средств. Обеспечивается вывод видеосигнала с выхода телевизионного или тепловизионного канала на внешний телемонитор в телевизионном стандарте.

## *Заключение*

Таким образом развитие оптико-электронных приборов (ОЭП) военного назначения привело к созданию комплексных систем разведки, в которых применяются приборы, основанные на использовании различных физических принципов – приборы ночного видения, приборы с телевизионными (ТВ), тепловизионными (ТпВ) и лазерными каналами. Основной предпосылкой комплексирования ОЭП является различное воздействие факторов естественного и искусственного происхождения на различные каналы получения видеоинформации, поскольку каждый из упомянутых каналов, взятый в отдельности, не в состоянии удовлетворять возросшим техническим требованиям в условиях плохой видимости, тщательной маскировки целей, активного применения средств радиоэлектронного противодействия.

При комплексировании ОЭП эффективность системы по дальности обнаружения целей оказывается выше эффективности каждого из каналов. При этом комплексирование происходит не только на основе конструктивно-технического объединения различных каналов, но и на основе частичного совмещения оптических осей, совместной обработки информации с целью ее одновременного представления на общем дисплее в виде единого изображения [4].

Анализ тенденций развития лазерных дальномеров показывает, что в будущем, благодаря развитию науки и техники, следует ожидать появления новых способов повышения точности, а также развития лазерных дальномеров по другим направлениям.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аснис Л. А., Васильев В. П., Волконский В. Б. и др. Лазерная дальнометрия / под общей редакцией В. П. Васильева и Х. В. Хиндрикус. – М.: Радио и связь, 1995. – 256 с.

2. Генике А. А., Афанасьев А. М. Геодезические свето- и радиодальномеры : учеб. для техникумов. – М.: Недра, 1988. – 302 с.

3. Комбаров М. С., Кузнецов М. М. Современные оптико-электронные средства наблюдения, разведки и прицеливания для стрелкового оружия нормального калибра // Интерэкспо ГЕО-Сибирь-2017. XIII Междунар. науч. конгр. : Национ. науч. конф. «Наука. Оборона. Безопасность-2017» : сб. материалов (Новосибирск, 17–21 апреля 2017 г.). – Новосибирск : СГУГиТ, 2017. – С. 104–107.

4. Мордвин Н. Н., Попов Г. Н. Концепция построения оптико-электронных приборов наблюдения универсального назначения / А. В. Голицын // Известия вузов. Приборостроение. - 2009. – Том 52, №6. - С. 34–39.

5. Методы модернизации лазерных дальномеров. Оборонный комплекс – научно-техническому прогрессу, № 2, 2010. – С. 59–62.

6. Чунарев Д.А., Давыдова Л.Г. Многоканальные приборы. Научно-технический журнал «Контенант». Том 14, № 4, 2015. – с.51-54.

7. Приборы ночного видения с фотоприемниками на основе InGaAs. – 2009. - № 2. [Электронный ресурс]. – Режим доступа: http://www.electronics.ru/.

8. Бардачевский Н.Н., Литовченко В.А. Применение лазерных дальномеров в военном деле // Интерэкспо ГЕО-Сибирь-2016. XII Междунар. науч. конгр. : Междунар. науч. конф. «Специальные вопросы фотоники: Наука. Оборона. Безопасность» : сб. материалов (Новосибирск, 18–22 апреля 2016 г.). – Новосибирск : СГУГиТ, 2016. – С. 78–84.

9. Оптико-электронные системы и лазерная техника. Энциклопедия [Текст] / под общей редакцией С. Б. Иванова. – М.: Оружие и технологии, 2005. – С. 325-327, 333.

10. Оптические и оптико-электронные приборы, системы прицеливания, разведки и наблюдения для сухопутных войск / [Предеин Л. П., Степанов А. М., Лукашевич В. К. и др.] / отв. ред.-сост. Малинин В. В. – Новосибирск: Наука, 2011. – 411 с.

11. Приборы ночного видения. Военные материалы. [Электронный ресурс]. – Режим доступа: http://50bmp.ru/.

12. Шилов, В., Гришанов, В. Лазер на военной службе. Армейский сборник. № 7, 2008. – С. 43 – 45.

13. Устиненко И. М., Можаев О. А. Состояние, перспективы развития и методы расчета характеристик лазерных дальномеров, целеуказателей и пеленгаторов лазерного пятна подсвета [Текст] / под общей редакцией В. А. Стефанова. – М.: Гос. НИИ авиац. Систем. Науч.-информ. центр. – 1991. – С. 4.

14. Развитие техники ночного видения: поколения ПНВ. http://www.laser-portal.ru/.

15. Волков В. Г. Портативные лазерные дальномеры. Специальная техника, № 6. 2001. – С. 2–9.

16. Бардачевский Н. Н., Литовченко В. А. Применение и развитие приборов ночного видеия в современной армии // Интерэкспо ГЕО-Сибирь-2017. XIII Междунар. науч. конгр. : Национ. науч. конф. «Наука. Оборона. Безопасность-2017» : сб. материалов (Новосибирск, 17–21 апреля 2017 г.). – Новосибирск : СГУГиТ, 2017. – С. 68–76.

17. Орлов В.А., Петров В.И. Приборы наблюдения ночью и при ограниченной видимости. – М.: Воениздат, 1989. – 256 с.

18. Грузевич Ю.К. Оптико-электронные приборы ночного видения. – М.: ФИЗМАТЛИТ, 2014. – 276 с. – ISBN 978-5-9221-1550-6.

19. Специальное конструкторское бюро техники ночного видения (СКБ ТНВ). Приборы и прицелы ночного видения в России. Истори*я* создания / Н. Ф. Кощавцев, Ю. Г. Эдельштейн, В. Г. Волков, А. А. Толмачев, С. Ф. Федотова, Т. К. Кирчевская [Электронный ресурс]. – Режим доступа: http://www.ak-info.ru/.

20. Отечественные приборы ночного видения. Армейский вестник. Интернет журнал. http://army-news.ru/.

УДК 528.022/535.3
DOI: 10.33764/2618-981X-2019-9-137-143

# ИССЛЕДОВАНИЕ ВЛИЯНИЯ АТМОСФЕРЫ НА РЕЗУЛЬТАТЫ ДАЛЬНОМЕРНЫХ ИЗМЕРЕНИЙ

***Болатбек Кожахметулы Бектанов***
Казахский национальный аграрный университет, 050010, Казахстан, г. Алматы, пр. Абая, 8, кандидат технических наук, профессор кафедры земельные ресурсы и кадастр, тел. 7(701)780-98-15, e-mail: bekbol53@yandex.ru

***Омар Абдуллаевич Сарыбаев***
Казахский национальный аграрный университет, 050010, Казахстан, г. Алматы, пр. Абая, 8, кандидат технических наук, профессор кафедры земельные ресурсы и кадастр, тел. 7(701)255-78-55, e-mail: sarybaev_o@mail.ru

***Гаухар Каналбековна Серикбаева***
Казахский национальный аграрный университет, 050010, Казахстан, г. Алматы, пр. Абая, 8, докторант кафедры земельные ресурсы и кадастр, тел. 7(707)345-47-24

***Азамат Бескемпирович Калдыбеков***
Казахский национальный аграрный университет, 050010, Казахстан, г. Алматы, пр. Абая, 8, докторант кафедры земельные ресурсы и кадастр, тел. 7(777)007-777-76

В статье описан метод, основанный на связи интегрального индекса преломления воздуха с его интегральным высотным градиентом. В условиях ограниченной по высоте атмосферы индекс преломления $N$ и его высотный градиент $dN/dH$ пропорциональны друг другу. Установлено, что градиенту индекса преломления можно найти сам индекс при известном коэффициенте связи между ними. При этом градиент легко найти по углу полной рефракции. Даны результаты экспериментальных исследований и рекомендации по его применению. Выполнен корреляционный анализ результатов синхронных измерений.

**Ключевые слова:** индекс преломления, высотный градиент, изотермия атмосферы, рефракционная траектория, корреляционный анализ, угол рефракции, светодальномерное измерение, безразмерные параметры.

# STUDY OF ATMOSPHERE INFLUENCE ON RESULTS OF DISTANCE MEASUREMENTS

***Bolatbek K. Bektanov***
Kazakh National Agrarian University, 8, Prospect Abay St., Almaty, 050010, Kazakhstan, Ph. D., Professor, Land Resources and Cadastre Department, phone: 7(701)780-98-15, e-mail: bekbol53@yandex.ru

***Omar A. Sarybayev***
Kazakh National Agrarian University, 8, Prospect Abay St., Almaty, 050010, Kazakhstan, Ph. D., Professor, Land Resources and Cadastre Department, phone: 7(701)255-78-55, e-mail: sarybaev_o@mail.ru

***Gauhar K. Serikbayeva***
Kazakh National Agrarian University, 8, Prospect Abay St., Almaty, 050010, Kazakhstan, Postdoc, Land Resources and Cadastre Department, phone: 7(707)345-47-24

***Azamat B. Kaldybekov***
Kazakh National Agrarian university, 8, Prospect Abay St., Almaty, 050010, Kazakhstan, Postdoc, Land Resources and Cadastre Department, phone: 7(777)007-777-76

The article describes a method based on the relationship of the integral index of refraction of air with its integral altitude gradient. The refractive index N and its altitude gradient dN / dH are proportional to each other under conditions of limited atmospheric height. It has been established that the gradient of the refractive index can be found by the index itself with a known coefficient of coupling between them. Wherein, it is easy to find the gradient by the angle of complete refraction. Results of experimental studies and recommendations for its use are given. A correlation analysis of the results of synchronous measurements was performed.

**Key words:** refractive index, altitude gradient, atmospheric isothermy, refraction trajectory, correlation analysis, refraction angle, luminoscopic measurement, dimensionless parameters.

Воздействие атмосферы на распространение оптического излучения приводит уменьшению скорости электромагнитных волн, что в свою очередь сказывается на результатах светодальномерных измерений. В настоящее время известен ряд методов решения проблемы повышения точности линейных измерений тождественной проблеме определения интегрального показателя преломления атмосферной среды вдоль измеряемой дистанции [1,2]. Наиболее перспективными из них можно признать интенсивно разрабатываемые инструментальные методы.

Вместе с тем как с практической, так и с научной точки зрения целесообразен поиск и других технических решений указанной проблемы.

Одним из них может служить подход, основанный на явлении изотермии атмосферы или обращения радиационного баланса в нуль, давно известный и вновь привлекший внимание исследователи [3-5]. На этом пути возникает задача определения моментов наступления изотермии с точностью до нескольких минут, которую можно решить с привлечением временной зависимости угла полной рефрации, найденного по взаимнообратным синхронно измеренным расстоянием на концах трассы. Момент наступления изотермии атмосферы соответствует в данном случае моменту, в который угол полной рефракции принимает значение, вычисленное по метеопараметрам [5].

Недостатком такого подхода является низкая производительность и точность, в связи с тем, что момент изотермии может и не паступить. С другой стороны, известен метод определения интегрального индекса преломления, включающий измерение взаимно обратных зенитных расстояний одновременно с измерением дальности [2,11]. Ограничения его точности также известны и заключаются в недостаточно полном соответствии индекса преломления, вычисленного по зенитным расстояниям. Дело в том, что можно предложить аналогичный путь решения проблемы, в основе которого также измерения зенитных расстояний одновременно со светодальномерными измерениями. Как показывают эксперименты, он более эффективен.

Сущность метода основана на связи интегрального индекса преломления воздуха с его интегральным высотным градиентом. В условиях ограниченной по высоте атмосферы индекс преломления $N$ и его высотный градиент $dN/dH$

пропорциональны друг другу. Рассмотрим зависимость индекса преломления от высоты

$$\mathrm{N}(H) = \mathrm{N}_0 exp(-CH) \tag{1}$$

где $N_0$ - индекс премломления по высоте $H_0$; $C$ - постоянный для данного $N_0$ коэффициент. После дифференцирования этого выражения будем иметь

$$\frac{dN(H)}{dN} = -CN(H) \tag{2}$$

Для угла полной рефракции можно записать уравнения:

$$\sigma = 10^{-6} L \int_0^1 \frac{dN(H)}{dH}(\xi) d\xi = -C10^{-6} L \int_0^1 N(H)(\xi) d\xi = -10^{-6} CL\overline{N}; \tag{3}$$

Поскольку угол полной рефракции равен сумме частных углов рефракции $r_1$ и $r_2$ в точках излучения и приема волны, т.е. они связаны функционально

$$r_1 = 10^{-6} L \int_0^1 \frac{dN(H)}{dH}(\xi)\xi d\xi = \frac{1}{2} 10^{-6} L \frac{d\widetilde{N}(H)}{dH}, \tag{4}$$

то можно получить и связь частных углов рефракции с индексом преломления в виде

$$r_1 = 10^{-6} C \frac{L}{2} \widetilde{N}. \tag{5}$$

В уравнении (4) обозначено $\xi = x/L$.

Таким образом, изложенное приводит к выводу о том, что градиенту индекса преломления можно найти сам индекс при известном коэффициенте связи между ними. При этом градиент легко найти по углу полной рефракции. Имея в виду поведение безразмерных параметров рефракционной траектории, состоящее в их статистическом постоянстве во времении [3] можно прийти к выводу, что аналогичным образом должны вести себя и отношения индексов преломления т.е.

$$\frac{\sigma}{r_1} = 2\frac{\overline{N}}{\widetilde{N}} - const \tag{6}$$

С учетом (6), можно записать

$$\frac{Ni(t)}{Nj(t)} = C_N - const; \qquad \frac{\widetilde{N}(t)}{Nij(t)} = \widetilde{C}_N, \tag{7}$$

что означает подобие законов изменения индексов преломленияв в двух выбранных точках.

Для экспериментального исследования отмеченного постоянства использованы результаты измерений, выполненных на Камчатке. На концах трассы различной длины измерялись метеопараметры, по которым по приближенной формуле вычислялись значения индексов преломления (табл. 1).

*Таблица 1*

Результаты расчета отношения индексов преломления

| Время наблюдения | $N'_1/N_2$ | Время наблюдения | $N'_1/N_2$ | Время наблюдения | $N'_1/N_2$ |
|---|---|---|---|---|---|
| Центр-Колдун L=750 м | | Караульный-Кратер L=11 793 м | | Центр-Скала L=17 848 м | |
| $11^h\ 45^m$ | 0, 9923 | $6^h\ 00^m$ | 1,0027 | $8^h\ 05^m$ | 0, 924 |
| 12 05 | 0, 9949 | 6 23 | 1,0000 | 8 14 | 0,9170 |
| 12 22 | 0, 9958 | 6 53 | 1,0006 | 8 30 | 0,9091 |
| 12 45 | 0, 9998 | 7 06 | 0,9988 | 8 45 | 0,9004 |
| 13 00 | 0, 9994 | 7 23 | 1,0027 | 9 04 | 0,8940 |
| 13 40 | 0, 9946 | 7 40 | 0,9985 | 9 13 | 0,8896 |
| 13 56 | 0, 9946 | | | | |
| 14 50 | 0, 9965 | | | | |
| 17 10 | 0, 9930 | | | | |

Из таблицы видно, что погрешность отношения показателя преломления $C_n$ ($C_N$) колеблется от $1\cdot10^{-6}$ до $1\cdot10^{-5}$. Этот факт подтверждает как гипотезу о сильной коррелированности или статистическом постоянстве во времени отношения индексов преломления.

Для нахождения коэффициента связи между $N(H)$ и $dN(H)/dH$ целесообразно использовать корреляционный анализ рядов синхронно измеренных параметров трассы. В этом случае коэффициент связи будет равен коэффициенту регрессии. Поскольку изменение измеряемого расстояния обусловено изменением интегрального индекса преломления, а изменения угла полной рефракции обусловлено изменением среднего по трассе градиента индекса преломления. Поэтому естественным является нахождение коэффициента связи между $L$ и σ, который будет тождествен коэффициенту связи между интегральными значениями $\tilde{N}(H)$ и $d\tilde{N}(H)/dH$. Таким образом, справедливо уравнение регрессии

$$L = \bar{L} + \hat{K}_{L\sigma}(\sigma - \bar{\sigma}), \tag{8}$$

где черта означает усреднение во времении, а для коэффициента регрессии уравнение

$$\hat{K}_{L\sigma} = \frac{\sum_{j=1}^{i}(L_j - \bar{L})(\sigma_i - \bar{\sigma})}{j \cdot m_\sigma^2}, \tag{9}$$

где $m_\sigma^2$ - дисперсия длиннопериодических изменений угла полной рефракции.

Уравнение (8) является основным и отражает физическую основу предлагаемой методики. По аналогии с этим уравнением можно также записать уравнение

$$L = \overline{L} + \hat{K}_{Lz}\left(Z' - \overline{Z}'\right), \tag{10}$$

которое вследствие существования зависимости $Z = Z_0 - r$ ($Z_0$ - истинное значение зенитного расстояния $Z$) тождественно уравнению

$$L = \overline{L} + \hat{K}_{Lr}\left(r' - \overline{r}'\right). \tag{11}$$

Для проверки справедливости уравнений (8) и (11) выполнен корреляционный анализ результатов синхронных измерений, проводившихся в различные годы на Камчатском геодинамическом полигоне - «Ключевском» и на геодезическом полигоне – «Чкалов» Московской области. В обработку при этом включались пары $L$ и $Z$ (табл. 2). Приведенные данные убедительно свидетельствуют о наличии связи между индексом преломления и его градиентом.

*Таблица 2*

Взаимосвязь дальности и зенитных расстояний

| Дальность $\overline{L}$, м | Зенитное расстояние $Z$ | Коэффициент корреляции $\rho_{ZL}$ | Число пар $j$ | Вероятность $P_0$ |
|---|---|---|---|---|
| 8 135 | $89^0$ 33' 09",8 | -0,74 | 5 | 0,80 |
| 4 232 | 98 35 27,8 | -0,81 | 6 | 0,95 |
| 4 003 | 88 33 58,0 | -0,68 | 10 | 0,99 |
| 14 346 | 88 35 18,2 | -0,31 | 10 | 0,95 |
| 9 887 | 87 03 49,2 | -0,76 | 8 | 0,99 |
| 15 869 | 89 42 06,6 | -0,84 | 9 | 0,99 |

Уравнения (8) и (10) пока не позволяют решить проблему определения интегрального индекса преломления в связи с отсутствием информации об абсолютном отклонении измеряемой дальности от истинного ее значения. Дальнейший путь заключается нахождении связи между вычисляемым и измеряемым метеопараметрам на концах трассы индексом преломления и углом полной рефракции с одной стороны и между индексом и дальностью с другой. Причем для вычисления индекса целесообразно использовать формулу Барелла-Сирса.

$$N = N_C \frac{T_C}{P_C}\frac{P}{T} + K\frac{e}{T}, \tag{12}$$

где $T_c$, $P_c$ - температура и давление воздуха при стандартных условиях; $K$ - известный коэффициент, зависящий от длины волны; $e$ - влажность.

Для разрешения неоднозначности воспользуемся моментом наступления изотермии атмосферы, не истинным а гипотетическим моментом. Другими словами, используем адиабатические условия. С этой целью в приведенных уравнениях необходимо место $\sigma$ использовать угол $\sigma_u$, соответствующий отмеченным условиям

$$\overline{\sigma}_u = 35{,}9 \cdot 10^{-4} \overline{P} \cdot \overline{T}^{-2} \cdot L. \tag{13}$$

Таким образом, реализация изложенного подхода включает следущие действия и условия.

1. Синхронные взаимно обратные измерения зенитных расстояний $Z_1$ и $Z_2$ одновременно с определением расстояния светодальномером, а также одновременным измерением метеопараметров на концах трассы.

2. Время измерений $t$ должно быть таким, чтобы изменение $L$, $\sigma$ и $N$ было существенным. Практически это время с учетом их суточного хода может быть 0,5 до 2 ч.

3. Корреляционный анализ, составление уравнений (8) и нахождение $L$ и $N$.

4. Вычисление метеорологической поправки в среднее значение расстояния $\overline{L}$ по формуле

$$L_M = \left(N_0 - N_И\right) \cdot 10^{-6} \cdot \overline{L},$$

где $L_0$ – постоянная светодальномера.

Следует отметить, что возможно использование и лишь односторонних зенитных расстояний, но в этом случае сложнее получение информации об угле рефракции в пункте наблюдения.

Таким образом, сущностью методики является переход от среднего значения индекса преломления <N> к интегральному $\widetilde{N}$ через коэффициент связи между ними. Погрешность определения коэффициента регрессии является основной для излагаемого метода и для ее оценки по формуле

$$m_{Kxy} \frac{m_x}{m_y} \frac{1 - \rho_{xy}^2}{\sqrt{j}}, \tag{14}$$

где $j$ - число пар $x$ и $y$.

Изложенное свидетельствует о возможности достижения точности $\sim(1 \div 3) \cdot 10^{-7}$ разработанным методом. Кроме того, еще раз подтверждена работоспособность метода определения угловой рефракции, основанного на корреляционной связи точечного и интегрального градиентов температур. Простое использование индексов $\overline{N}_1$ или $\overline{N}_{ср}$ к точности лишь $\sim 1{,}3 \cdot 10^{-6}$.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Учет атмосферных влияний на астрономо-геодезические измерения / Островский А. Л., Джуман Б. Н., Заблоцкий Ф. Д. и др. – М. : Недра, 1990.

2. Виноградов В. В. Влияние атмосферы на геодезические измерения. – М. : Недра, 1992.

3. Дементьев В. Е. Исследование вертикальной рефракции на горизонтальных трассах в аридной зоне // Геодезия и картография. - 2014, - №2, - С. 57-64. ISSN 0016 - 7126.

4. Вшивкова О.В. Повышение качества планировочных работ посредством учета влияния атмосферы // Изв. вузов Геодезия и картография. - 2010, - №5, - С. 3-5, ISSN 0536 - 101X.

5. Вшивкова О.В. Учет влияния атмосферы в электронной тахеометрии с использованием геодезического градиентометра // Изв. вузов «Геодезия и аэрофотосъемка». – 2010. – № 3.

6. Ефимов В.О. Оптическая рефракция и модельные методы учета ее влияния на характеристики дальномерного тракта лазерного локатора слежения // Инженерный вестник Дона, 2017, №3 URL: ivdon.ru/magazine/archive/n3y2017/2248/.

7. Федянин М.Р., Лазеров В.М. Фотограмметрическая рефракция в модели однородной атмосферы // Международный научно-исследовательский журнал. – 2017. – №1(55).

8. Быкасов Д.А., Водкайло Е.Г. Устранение влияния атмосферной рефракции на примере определения широты места по Солнцу // Молодой ученый. – 2017. – № 19. – С. 10-13.

9. Ефимов В.О., Пикулев А.Н., Дорогов Н.В. и др. Оптическая рефракция и модельные методы учета ее влияния на характеристики дальномерного тракта лазерного локатора слежения // Инженерный вестник Дона. – 2017. – № 3.

10. Островский А.Л. Достижения и задачи рефрактометрии. Геопрофи. – 2008. – № 1.

11. Бектанов Б.К., Есимова К.А., Балкожа М.А. Способ определения вертикальных углов рефракции. Патент на полезную модель. – №1737. – БИ №12. – 2016.

12. Nordblad E., Leyser T.B. Ray tracing analysis of L mode pumping of the ionosphere, with implication for magnetic zenith effect //Ann. Geophys. 2010. V. 28. P. 1749−1759.

13. Rietveld M.T., Kosch M.J., Blagiveshcenskaya N.F. et al. Ionospheric electron heating, aurora and striations induced by powerful HF radio waves at high latitudes: aspect angle dependence // J. Geophys. Res. 2003. 108(A4). 1141.

14. Kosch M. J., Pedersen T., Mishin E. et al. Temporal Evolution of Pump Beam Self-Focusing at the High-Frequency Active Auroral Research Program // J. Geophys. Res. 2007. V. 112. A8 304.

15. Eugene Levin, Dmitry Mozer, Jessica Mc Carty. Comparative Analysis of Software Packages for RADAR Data Interferometric Processing from CIS Country View. Surveying and Land Information Systems (SaLIS), Ed. Steve Frank, (in Press for Nov 2017 -Issue). Impact factor=1.3.

## СОДЕРЖАНИЕ

## CONTENTS

*Научное издание*

# ИНТЕРЭКСПО ГЕО-СИБИРЬ

XV Международный научный конгресс

Сборник материалов в 9 т.

Т. 9
Национальная конференция

**«НАУКА. ОБОРОНА. БЕЗОПАСНОСТЬ-2019»**

Материалы публикуются в авторской редакции

Компьютерная верстка *Н. Ю. Леоновой*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 20.11.2019. Формат 60 × 84 1/16.
Усл. печ. л. 8,60. Тираж 33 экз. Заказ 176.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.