

ISSN 2658-3593 (Print)
ISSN 2713-1564 (Online)

**N
B TECHNOLOGIES**
I

NANO / BIO / INNOVATION TECHNOLOGIES

Volume 14. No. 4

2020

Том 14. № 4

**Н
Б ТЕХНОЛОГИИ**
И

НАНО / БИО / ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ

ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

VOLGOGRAD STATE UNIVERSITY

ISSN 2658-3593 (Print)
ISSN 2713-1564 (Online)



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Н
Б ТЕХНОЛОГИИ
И Нано / Био / Инновационные технологии

2020
Том 14. № 4

MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE RUSSIAN FEDERATION

N
B TECHNOLOGIES
I Nano / Bio / Innovation Technologies

2020
Volume 14. No. 4



NBI TECHNOLOGIES

2020. Vol. 14. No. 4

Academic Periodical

First published in 2006

4 issues a year

Founder:

Federal State Autonomous
Educational Institution
of Higher Education
“Volgograd State University”

The journal is registered in the Federal Service for Supervision of Communications, Information Technology and Mass Media (Registration Number **ПН № ФС77-73361** of July 24, 2018)

The journal is included into the **Russian Science Citation Index**

The journal is also included into the following Russian and international databases: **CrossRef** (USA), **DOAJ** (Sweden), **ProQuest** (USA), **Google Scholar** (USA), **JournalSeek** (USA), **OCLC WorldCat®** (USA), **SHERPA/ROMEO** (Spain), **ULRICHSWEB™ Global Serials Directory** (USA), **VINITI Database RAS** (Russia), “**CyberLeninka**” **Scientific Electronic Library** (Russia), “**Socionet**” **Information Resources** (Russia), **IPRbooks E-Library System** (Russia), **E-Library System “University Online Library”** (Russia)

Editorial Staff:

Prof., Dr. *I.V. Zaporotzkova* – Chief Editor (Volgograd)
Assoc. Prof., Cand. *Yu.S. Bakhracheva* – Executive Secretary and Copy Editor (Volgograd)

Editorial Board:

Prof. *Alberto D'Amore* (Aversa, Italy); Prof. *Alfonso Jimenez* (Alicante, Spain); Prof., Dr. *V.A. Babkin* (Mikhaylovka); Prof., PhD *Bob A. Howell* (Mount Pleasant, USA); Prof., Dr. *D.P. Frolov* (Volgograd); Prof. *Jan Pielichowski* (Krakow, Poland); Prof., Dr. *K. Friedrich* (Kaiserslautern, Germany); Prof., Dr. *S.V. Krasnov* (Tolyatti); Prof., Dr. *I.Yu. Kvyatkovskaya* (Astrakhan); Prof., PhD *LinShu Liu* (Wyndmoor, USA); Prof. *Slavcho Kirillov Rakovsky* (Sofia, Bulgaria); Prof. *Victor Manuel de Matos Lobo* (Coimbra, Portugal); Prof., Dr. *G.E. Zaikov* (Moscow)

Editor of English texts *Yu.V. Chemeteva*

Making up: *Yu.A. Uskova*

Technical editing: *N.M. Vishnyakova, O.N. Yadykina*

Passed for printing: Dec. 23, 2020.

Date of publication: Mar. 23, 2021.

Format 60×84/8. Offset paper. Typeface Times.

Conventional printed sheets 4.6. Published pages 4.9.

Number of copies 500 (1st duplicate 1–47).

Order . «C» 45.

Open price

Address of the Printing House:
Bogdanova St, 32, 400062 Volgograd.

Postal Address:

Prosp. Universitetsky, 100, 400062 Volgograd.
Publishing House of Volgograd State University.
E-mail: izvolgu@volsu.ru

Address of the Editorial Office and the Publisher:

Prosp. Universitetsky, 100, 400062 Volgograd.

Volgograd State University.

Tel.: (8442) 46-03-68, 46-55-99. Fax: (8442) 46-18-48

E-mail: vestnik10@volsu.ru

Journal website: <https://ti.jvolsu.com>

English version of the website:

<https://ti.jvolsu.com/index.php/en/>

НБИ ТЕХНОЛОГИИ

2020. Т. 14. № 4

Научно-теоретический журнал

Основан в 2006 году

Выходит 4 раза в год

Учредитель:

Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет»

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (регистрационный номер **ПИ № ФС77-73361** от 24 июля 2018 г.)

Журнал включен в базу **Российского индекса научного цитирования (РИНЦ)**

Журнал также включен в следующие российские и международные базы данных: **CrossRef** (США), **DOAJ** (Швеция), **ProQuest** (США), **Google Scholar** (США), **JournalSeek** (США), **OCLC WorldCat®** (США), **SHERPA/RoMEO** (Испания), **ULRICHSWEB™ Global Serials Directory** (США), **ВИНИТИ** (Россия), **Научная электронная библиотека «КиберЛенинка»** (Россия), **Соционет** (Россия), **Электронно-библиотечная система IPRbooks** (Россия), **Электронно-библиотечная система «Университетская библиотека онлайн»** (Россия)

Редакционная коллегия:

д-р физ.-мат. наук, проф. *И.В. Запороцкова* – главный редактор (г. Волгоград)
канд. техн. наук, доц. *Ю.С. Бахрачева* – ответственный и технический секретарь (г. Волгоград)

Редакционный совет:

проф. *Алберто Д'Аморэ* (г. Аверса, Италия); проф. *Альфонсо Хименес* (г. Аликанте, Испания); д-р хим. наук, проф. *В.А. Бабкин* (г. Михайловка); проф., PhD *Боб А. Ховелл* (г. Маунт-Плезант, США); д-р экон. наук, проф. *Д.П. Фролов* (г. Волгоград); проф. *Ян Пиеличовский* (г. Краков, Польша); д-р, проф. *К. Фридрих* (г. Кайзерслаутерн, Германия); д-р техн. наук, проф. *С.В. Краснов* (г. Тольятти); д-р техн. наук, проф. *И.Ю. Квятковская* (г. Астрахань); проф., PhD *Лин Шу Лиу* (г. Уиндмур, США); проф. *Славчо Кириллов Раковский* (г. София, Болгария); проф. *Виктор Мануэль де Матос Лобо* (г. Коимбра, Португалия); д-р хим. наук, проф. *Г.Е. Заиков* (г. Москва)

Редактор английских текстов *Ю.В. Чеметева*

Верстка *Ю.А. Усковой*

Техническое редактирование *Н.М. Вишняковой,*

О.Н. Ядыкиной

Подписано в печать 23.12 2020 г.

Дата выхода в свет: 26.03 2021 г.

Формат 60×84/8. Бумага офсетная. Гарнитура Таймс.

Усл. печ. л. 4,6. Уч.-изд. л. 4,9.

Тираж 500 экз. (1-й завод 1–47 экз.).

Заказ . «С» 45.

Свободная цена

Адрес типографии:

400062 г. Волгоград, ул. Богданова, 32.

Почтовый адрес:

400062 г. Волгоград, просп. Университетский, 100.

Издательство

Волгоградского государственного университета.

E-mail: izvolgu@volsu.ru

Адрес редакции и издателя:
400062 г. Волгоград, просп. Университетский, 100.
Волгоградский государственный университет.
Тел.: (8442) 46-03-68, 46-55-99. Факс: (8442) 46-18-48
E-mail: vestnik10@volsu.ru
Сайт журнала: <https://ti.jvolsu.com>
Англояз. сайт журнала:
<https://ti.jvolsu.com/index.php/en/>

СОДЕРЖАНИЕ

Запороцкова И.В. Обращение главного редактора 5

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

Бабенко А.А., Бахрачева Ю.С., Алеева А.Р.
Система фильтрации нежелательных приложений
интернет-ресурсов 6

Демьянов Г.Д., Садовникова Н.П. Система
контроля взаимодействия в сети
с подключением IoT-устройств 12

Запороцков П.А. Разработка
метода проведения аудита
системы технической защиты информации 18

ИННОВАЦИИ В МЕТАЛЛУРГИИ И МАТЕРИАЛОВЕДЕНИИ

Васильев А.В., Афанасьев А.М. Исследование
физико-механических свойств
радиопоглощающих материалов [*На англ. яз.*] 28

*Кожитов Л.В., Запороцкова И.В., Борознина Н.П.,
Борознин С.В., Акатьев В.В.* Исследование
взаимодействия углекислого газа
с модифицированными функциональными группами
нанотрубок 33

Какорина О.А., Какорин И.А., Панченко А.Н.
Выявление примесей в воде
с помощью наноструктур 39

CONTENTS

Zaporotskova I.V. Editor's Foreword 5

INNOVATIONS IN INFORMATICS, COMPUTING AND MANAGEMENT

Babenko A.A., Bahracheva Yu.S., Aleeva A.R.
System for Filtering Unwanted Applications
of Internet Resources 6

Demyanov G.D., Sadovnikova N.P. Network
Interaction Monitoring System
with IoT Devices Connected 12

Zaporotskov P.A. Development
of a Method for Conducting an Audit
of the Information Security System 18

INNOVATIONS IN METALLURGY AND MATERIALS SCIENCE

Vasiliev A.V., Afanasiev A.M. Investigation
of the Physical and Mechanical Properties
of Radio-Absorbing Materials 28

*Kozhitov L.V., Zaporotskova I.V., Boroznina N.P.,
Boroznin S.V., Akatiev V.V.* Investigation
of the Interaction of Carbon Dioxide
with Modified Functional Groups
of Nanotubes 33

Kakorina O.A., Kakorin, I.A., Panchenko A.N.
Detection of Impurities in Water
Using Nanostructures 39

Обращение главного редактора

Дорогие друзья, авторы и читатели нашего журнала!

В этом году на мировом рынке технологий произошли глубокие структурные изменения, причиной которых является насыщение высокотехнологичных отраслей принципиально новыми методами обработки. Пандемия коронавируса, плачевно сказавшаяся на многих традиционных отраслях, создала новые возможности и ниши для научных разработок в области информационных и новых производственных технологий. Эта тенденция привела к необходимости оценки снижения технологических рисков при внедрении таких технологий. Одно из основных условий внедрения инноваций – наличие инфраструктуры, осуществляющей связь предприятия-разработчика с конечными потребителями с целью постоянного выявления новых требований покупателей, предъявляемых к качеству производимых товаров и услуг. Нано-, био-, информационные технологии органично дополняют и активно влияют друг на друга. Наш журнал предназначен освещать широкий спектр научных проблем, связанных с решением актуальных вопросов в сфере науки, техники и инноваций.

Каким станет для нас 2021 год, что он нам принесет, зависит от многого, но в первую очередь – от нас. Убеждена, что вера в свои силы, ответственность, энтузиазм помогут осуществить все планы, сделать нашу жизнь более насыщенной и интересной. Пусть в Новом году вас ждет творческий поиск, который обязательно увенчается ярким и важным результатом. Желаю жизненной энергии и интересных профессиональных событий, чтобы ваши новые статьи появились на страницах журнала.

И.В. Запороцкова,
доктор физико-математических наук, профессор,
директор института приоритетных технологий ВолГУ



ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.1>

УДК 004.738.5:004.42

ББК 32.972.53

СИСТЕМА ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНЫХ ПРИЛОЖЕНИЙ ИНТЕРНЕТ-РЕСУРСОВ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
ba_benko@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
bakhacheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Романовна Алеева

Студент кафедры информационной безопасности,
Волгоградский государственный университет
bakhacheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Был разработан проект программного комплекса фильтрации интернет-трафика на языке программирования C# и описаны его функциональные возможности. В результате проведенных экспериментов системой фильтрации были: удачно проверена корректность работы фильтрации по DNS-записи, удачно проверена корректность работы фильтрации по URL-адресу, сформированы отчеты о выявленных заблокированных сайтах в журнале фильтрации. Таким образом успешное проведение экспериментов позволяет утверждать о выполнении про-

граммного комплекса контент- фильтрации интернет-трафика поставленных перед ним задач.

Ключевые слова: интернет-трафик, фильтрация, конфиденциальная информация, информационная безопасность, программный комплекс.

Необходимость фильтрации интернет-трафика возникает, как и дома, так и для корпоративных сетей. Неограниченный доступ к интернету повышает шанс заражения ПЭВМ вредоносным программным обеспечением, фишинговым атакам и т.п. Второй проблемой, возникающей как в следствии внешних атак, заражения вредоносным программным обеспечением, так и в следствии действий внутреннего злоумышленника (или нарушителя, в т. ч. и неосознанного) – утечка конфиденциальной информации в следствии доступа к Интернет [7].

Согласно исследованию, реальный трафик в Интернете за 10 минут от средней корпоративной сети содержал приблизительно 57 000 пакетов, 1 100 сеансов и 26 протоколов. Большая часть трафика приходится на TCP-протоколы. Причем порты соединений – 80 и 443, которые чаще всего ассоциированы с протокола HTTP или HTTPS/TLS. Причем именно эти 2 протокола составляют большую часть трафика, относящуюся к web-трафику (то есть использование пользователями web-браузеров) [2].

Анализ результатов содержимого интернет-трафика по информации, содержащейся в нем, показал, что среди интернет-трафика наиболее часто встречающимся является протокол HTTP, причем если рассматривать передаваемое содержимое, то большая часть трафика приходится на видео-трафик и web-контент [1; 4].

В результате анализа назначения фильтрации интернет-трафика с целью выбора подходящего вида фильтрации интернет-трафика было выделено 3 вида фильтрации [3; 5; 6; 8]:

- 1) пакетная фильтрация;
- 2) фильтрация по протоколам прикладного уровня;
- 3) фильтрация по контенту.

Для дальнейшей работы был выбран метод фильтрации по контенту.

Были проанализированы системы и методы контент-фильтрации, а также определена их применимость для каждого из каналов утечки информации: блокирование по IP-адресу, блокировка по DNS-записи, блокирование по URL-адресу, фильтрация по текстовому содержимому, фильтрация по расширениям и типам файлов, фильтрация результатов поиска.

В результате были выбраны два метода: блокировка по DNS-записи и блокировка по URL-запросу.

Разработка формализованной модели программного комплекса фильтрации интернет-трафика

Процесс блокировки по URL-адресам представляет собой:

$$Den_{URL} = \begin{cases} u_i \in U^D, \text{ ресурс подлежит блокировке} \\ u_i \notin U^D, \text{ ресурс не подлежит блокировке} \end{cases}$$

Процесс блокировки по DNS-именам представляет собой:

$$Den_{DNS} = \begin{cases} d_i \in D^D, \text{ ресурс подлежит блокировке} \\ d_i \notin D^D, \text{ ресурс не подлежит блокировке} \end{cases}$$

Множество URL-адресов $U = \{u_1, \dots, u_n\}$, где URL-адрес u_i представляется двойкой:

$$u_i = (d_i, p_i),$$

где d_i – доменное имя в URL-адресе, p_i – путь запроса в URL-адресе.

Множество доменных имен (DNS-записей) $D = \{d_1, \dots, d_m\}$, где $m \leq n$,

Множество запрещенных URL-адресов $U^D = \{u_1^D, \dots, u_n^D\}$,

Множество запрещенных DNS-имен $D^D = \{d_1^D, \dots, d_m^D\}$.

Разработка архитектуры программного средства, реализующего программный комплекс фильтрации интернет-трафика

Архитектура программного комплекса, состоит из 6 основных модулей: модуль пользовательского интерфейса, модуль настройки, модуль отчета, модуль анализа трафика, модуль работы с трафиком, модуль базы данных запрещенных / разрешенных DNS, URL.

Архитектура программного комплекса представлена на рисунке 1 и в таблице.

Разработка алгоритмов работы программного комплекса фильтрации интернет-трафика

Программный комплекс фильтрации интернет – трафика предусматривает два метода фильтрации:

- 1) фильтрация по DNS-именам,
- 2) фильтрация по URL-адресу.

В первом случае сайт блокируется, если этот сайт находится в списке DNS-имен, которые следует блокировать.

Во втором случае страница сайта блокируется, если она находится в списке URL-адресов которые следует блокировать.

Описанные выше методы фильтрации легко формализовать в виде блок-схем, представленной на рисунке 2.

Блок-схема описывает обобщенный алгоритм фильтрации, включающий следующие шаги:

- 1) на втором шаге после ввода URL-адреса, загружается веб-страница;
- 2) на третьем шаге происходит фильтрация по DNS и URL;
- 3) на четвертом вывод результата: либо веб-страница заблокирована, либо страница загружается в первоначальном виде.

Далее был разработан проект программного комплекса фильтрации интернет-трафика на языке программирования C# и описаны его функциональные возможности.

Было проведено 3 экспериментальных исследования. В результате проведенных экспериментов системой фильтрации были: удачно проверена корректность работы фильтрации по DNS-записи, удачно проверена корректность работы фильтрации по

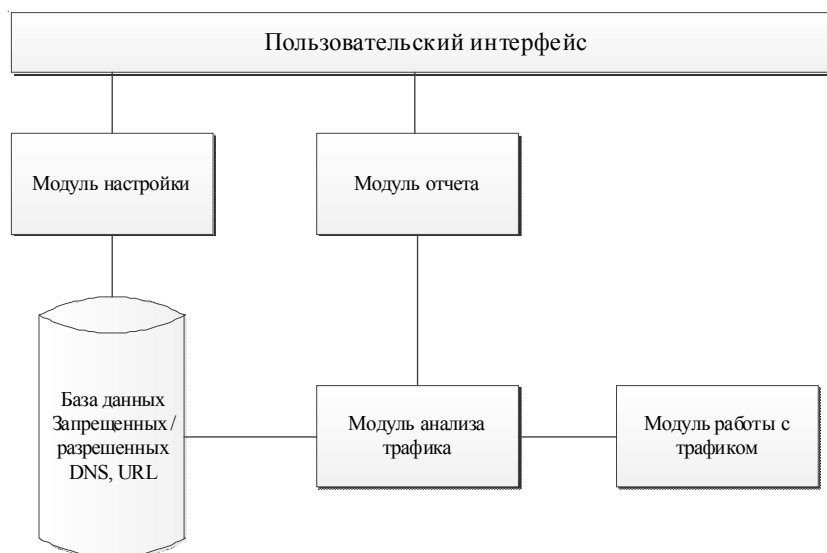


Рис. 1. Архитектура программного средства контент-фильтрации

Составные части архитектуры программного комплекса

Настройка	Состоит из создания и удаления списков доступа и по которым следует блокировать сайт
Анализ трафика	Выполняет анализ трафика на допуск к ним
Работа с трафиком	Выполняет задачу блокирования сайта
Отчет	Выводит список сайтов, к которым запрещен доступ

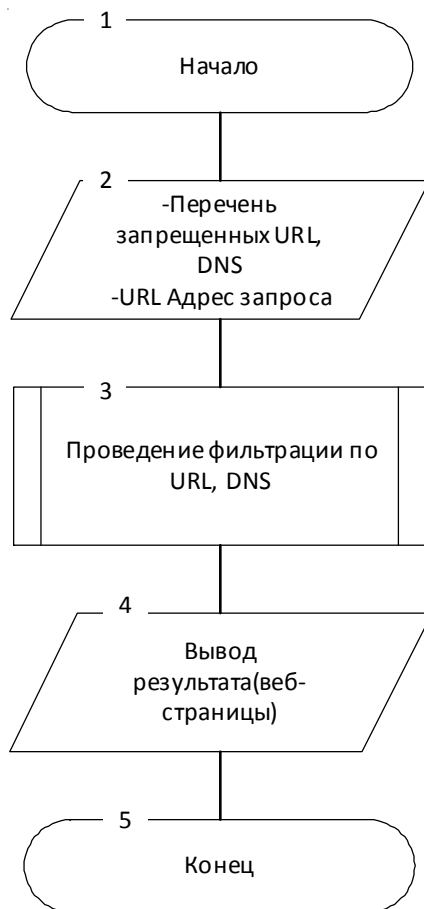


Рис. 2. Блок-схема алгоритма работы программного комплекса фильтрации интернет-трафика

URL-адресу, сформированы отчеты о выявленных заблокированных сайтах в журнале фильтрации.

Таким образом, успешное проведение экспериментов позволяет утверждать о выполнении программного комплекса контент-фильтрации интернет-трафика поставленных перед ним задач.

СПИСОК ЛИТЕРАТУРЫ

1. Лапони́на, О. Р. Межсетевое экранирование / О. Р. Лапони́на. – М. : Бином. Лаборатория знаний, 2007. – 343 с.
2. Медведовский, И. Д. Атака на Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – 2-е изд., перераб. и доп. – М. : ДМК, 2002. – 336 с.
3. Политики доступа и фильтрация трафика. – Электрон. текстовые дан. – Режим доступа: <http://help.smart-soft.ru/index.html?howworkfilter.htm> (дата обращения: 20.09.2020). – Загл. с экрана.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изм. и доп. в ред. от 13.07.2015). – Доступ из справ.-правовой системы «КонсультантПлюс».
5. Фильтрация DNS запросов. – Электрон. текстовые дан. – Режим доступа: <https://ospfripe.livejournal.com/2194.html> (дата обращения: 23.09.2020). – Загл. с экрана.
6. Фильтрация HTTPS трафика. – Электрон. текстовые дан. – Режим доступа: <https://www.carbonsoft.ru/фильтрация-https-трафика> (дата обращения: 20.09.2020). – Загл. с экрана.
7. Чемодуров, А. С. Обзор средств фильтрации трафика в корпоративной сети / А. С. Чемодуров, А. Ю. Карпутина // Научно-методический электронный журнал «Концепт». – 2015. – № 2. – Электрон. текстовые дан. – Режим доступа: <http://e-koncept.ru/2015/15039.htm>. – Загл. с экрана.
8. URL-фильтрация или как пользователю ограничить доступ в интернет. – Электрон. текстовые дан. – Режим доступа: <https://club.dns-shop.ru/forum/thread/46735> (дата обращения: 20.09.2020). – Загл. с экрана.

REFERENCES

1. Laponina O.R. *Mezhsetevoe ekranirovanie* [Firewall Protection]. Moscow, Binom. Laboratoriya znaniy, 2007. 343 p.

2. Medvedovskij I.D., Sem'yanov P.V., Leonov D.G. *Ataka na Internet* [Attack on the Internet]. Moscow, DMK Publ., 2002. 336 p.

3. *Politiki dostupa i fil'traciya trafika* [Access Policies and Traffic Filtering]. URL: <http://help.smartsoft.ru/index.html?howworkfilter.htm> (accessed 20 September 2020).

4. *Federal'nyj zakon "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" ot 27.07.2006 № 149-FZ (s izm. i dopol. v red. ot 13.07.2015)* [Federal Law "About Information, Information Technologies and Information Protection" of 27 July 2006 no. 149-FZ (as Amended

and Supplemented on 13 July 2015)]. Access from Reference Legal System "KonsultantPlyus".

5. *Fil'traciya DNS zaprosov* [DNS Query Filtering]. URL: <https://ospf-ripe.livejournal.com/2194.html> (accessed 23 September 2020).

6. *Fil'traciya HTTPS trafika* [Filtering HTTPS Traffic]. URL: <https://www.carbonsoft.ru/fil'traciya-https-trafika> (accessed 20 September 2020).

7. Chemodurov A.S., Karputina A. Yu. *Obzor sredstv fil'tracii trafika v korporativnoj seti* [Overview of Traffic Filtering Tools in the Corporate Network]. *Nauchno-metodicheskij elektronnyj zhurnal «Koncept»*, 2015, no. 2. URL: <http://e-koncept.ru/2015/15039.htm>.

8. *URL fil'traciya ili kak pol'zovatelyu ogranichit' dostup v internet* [URL Filtering or How to Restrict User Access to the Internet]. URL: <https://club.dns-shop.ru/forum/thread/46735> (accessed 20 September 2020).

SYSTEM FOR FILTERING UNWANTED APPLICATIONS OF INTERNET RESOURCES

Alexey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Information Security,
Volgograd State University
ba_benko@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Yulia S. Bahracheva

Candidate of Sciences (Engineering), Associate Professor, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina R. Aleeva

Student, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru 100
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Currently, the role of the Internet in the life of society is growing, and the state's view of it is changing. Increasingly, the content posted on the Web goes beyond the laws of individual countries, their social norms, and the political lines of the authorities. Besides, Internet has a significant impact on intellectual property and telecommunications, jeopardizing the economic interests of many industries. These trends have contributed to the need to filter some types of content, and have caused disputes about the permissible limits of state intervention in the functioning of the network. Content filtering systems and methods were analyzed, and their applicability for each of the information leakage channels was determined: blocking by IP address, blocking by DNS record, blocking by URL, filtering by text content, filtering by

extensions and file types, filtering search results. The project of a software package for filtering Internet traffic in the C# programming language was developed and its functionality was described. As a result of the experiments carried out by the filtering system, the following results were obtained: the correctness of filtering by DNS record, the correctness of filtering by URL were successfully checked, reports on identified blocked sites in the filtering log were generated. Thus, the successful conduct of experiments allows us to assert that the software package of content filtering of Internet traffic performs the tasks assigned to it.

Key words: Internet traffic, filtering, confidential information, information security, software package.



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.2>

УДК 004.056.53

ББК 32.971.35

СИСТЕМА КОНТРОЛЯ ВЗАИМОДЕЙСТВИЯ В СЕТИ С ПОДКЛЮЧЕНИЕМ IoT-УСТРОЙСТВ

Глеб Дмитриевич Демьянов

Студент кафедры информационной безопасности,
Волгоградский государственный университет
005_gleb@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Наталья Петровна Садовникова

Доктор технических наук, профессор кафедры «Системы автоматизированного проектирования и поискового конструирования»,
Волгоградский государственный технический университет
npsn1@yandex.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Аннотация. В статье рассматривается вопрос использования системы контроля взаимодействия в сети с подключением IoT-устройств. Выделяются основные угрозы информационной безопасности IoT-устройств и методы защиты представленных угроз. Посредством анализа выбирается приоритетный метод защиты и описывается как этот метод можно реализовать на практике.

Ключевые слова: интернет вещей, IoT-устройства, контроль взаимодействия в сети, информационная безопасность.

Интернет вещей (англ. internet of things, IoT) – концепция вычислительной сети физических предметов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей, как явление, способное перестроить экономические и общественные процессы, исключаяющее из части действий и операций необходимость участия человека [1].

Технология IoT оказала существенное влияние на развитие информационных технологий и других отраслей. Согласно Forbes, ожидается, что рынок интернет вещей в 2021 году достигнет 520 млрд долларов по сравнению с 235 млрд долларов в 2017 году,

что свидетельствует о непрерывном росте потребности в таких устройствах в будущем [5]. Также, по оценкам Gartner Research, количество устройств, подключенных к Интернету, к 2021 году достигнет 25 миллиардов по сравнению с 8,4 миллиарда в 2017 году [4].

С каждым годом будет расти как количество устройств IoT, так и количество злоумышленников. Лаборатория Касперского представила следующую статистику за 2016–2018 годы [2] (см. рис. 1).

К основным типам угроз можно отнести (см. табл. 1):

На основе анализа угроз можно выделить основные методы защиты устройств IoT [3]:

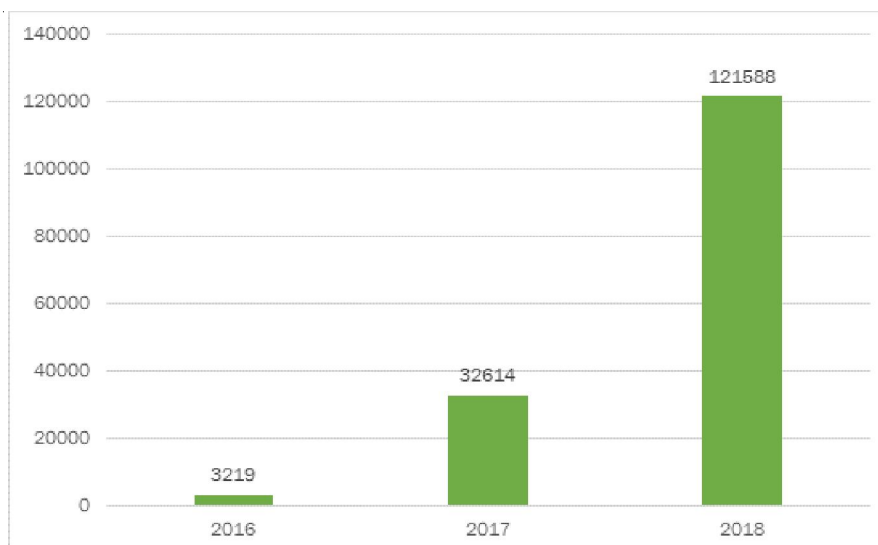


Рис. 1. Количество образцов вредоносного ПО для IoT-устройств в коллекции «Лаборатории Касперского», 2016–2018 гг.

Таблица 1

Анализ основных угроз, связанных с подключением устройств IoT

Субъект угрозы	Объект угрозы
Ботнеты и атаки DDoS	Сетевые ресурсы
Удаленная запись данных, передаваемых устройством	Конфиденциальные данные пользователя
Ransomware	Пользователь, имущество пользователя
Реальные кражи (взлом умных замков, автомобилей, гаражных дверей)	Пользователь, имущество пользователя

1. Безопасность связи – использование технологий шифрования, проверки подлинности.

2. Защита устройств – использование технологий обеспечения безопасности и целостности программного кода.

3. Контроль устройств – поддержка уже созданных устройств, выпуск обновлений прошивки, патчей, закрывающие бреши в защите прошлых патчей.

4. Контроль взаимодействия в сети – проанализировав все методы, приведенные выше, я пришел к выводу, что именно этот метод является самым надежным для обнаружения и предотвращения атаки на устройство. Контроль и защита устройств остается на стороне разработчика этих устройств, а безопасность связи и контроль взаимодействия в сети – на стороне предприятия использующего устройства IoT.

Наряду с эффективностью метода защиты так же можно выделить такой важный критерий выбора, как стоимость реализации метода защиты. В связи с этим самым перспек-

тивным направлением защиты является контроль взаимодействия в сети.

Было проанализировано несколько средств контроля взаимодействия в сети без использования IoT-технологий. Основой для этих программных средств является предупреждение пользователя о вероятном злоумышленнике, подключившимся к сети (см. табл. 2).

Для защиты устройств IoT необходимо выделять такие потенциально опасные подключения в отдельную группу и контролировать их деятельность в сети. Поэтому основными функциями системы контроля взаимодействия в сети должны быть анализ деятельности потенциально опасных устройств в сети и обнаружение новых потенциально опасных подключений.

Анализ действий в сети будет осуществляться посредством анализа заголовка каждого пакета в сети, основным сигналом к анализу передаваемых данных послужат поля заголовка «адрес получателя» и «адрес отправителя» (см. рис. 2).

Методы контроля взаимодействия в сети

Наименование программы	Возможность автоматического сканирования устройств в сети	Информация об устройстве	Логирование	Обнаружение новых подключений
Wi-Fi Network Monitor	Есть	Показывает IP-адрес, MAC-адрес, имя устройства	Сохраняет отчет в форматах HTML/XML/CSV/TXT	Есть
SoftPerfect WiFi Guard	Есть	Показывает IP-адрес, MAC-адрес, имя, пинг устройства	Нет	Есть

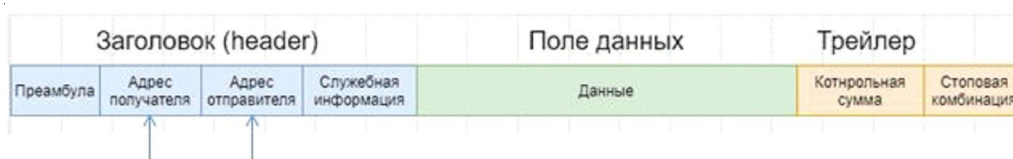


Рис. 2. Структура пакета, передаваемого по сети

Обнаружение новых подключений будет осуществляться посредством мониторинга подключенных устройств в сети и ведения списков уже подключенных устройств.

Для получения пакетов отдельным устройством, на котором будет проходить анализ подключений и действий в сети, нужно будет использовать одну из представленных ниже технологий перехвата пакетов в сети (табл. 3).

Вне зависимости от выбора технологии зеркалирования пакетов, разрабатываемая система будет работать с этими пакетами. Проанализировав все три технологии, можно сделать вывод, что наиболее удобными будут технологии SPAN и RSPAN. Значитель-

ный минус технологии TAP – необходимость устанавливать в сеть специального оборудования и, в следствии чего, невозможность удаленной настройки.

Можно выделить следующие основные функции системы контроля взаимодействия в сети:

1. Сканирование подключенных к сети устройств.
2. Ведение списков доверенных устройств, устройств IoT и потенциально опасных устройств.
3. Перехват пакетов потенциально опасных устройств.
4. Анализ пакетов на наличие вредоносных действий в сторону IoT-устройств.

Таблица 3

Анализ популярных средств перехвата пакетов по сети

Название технологии	Потеря пакетов	Удобство настройки	Сложность установки
SPAN (port mirroring)	Потеря пакетов незначительна, но присутствует	Можно фильтровать зеркалируемые пакеты, уменьшая объем данных. Можно настроить отражаемую сеть VLAN	Необходимо наличие коммутатора, поддерживающего технологию SPAN
RSPAN	Потеря пакетов незначительна, но присутствует	Можно фильтровать зеркалируемые пакеты, уменьшая объем данных. Можно настраивать отражаемую сеть VLAN и принимающую сеть VLAN	Необходимо наличие коммутатора, поддерживающего технологию RSPAN
TAP (Test Access Point)	Практически без потери	TAP – аппаратное средство и его необходимо размещать непосредственно в сети, а не задавать настройками коммутатора, нет возможности поменять настройки удаленно	Необходимо наличие, помимо коммутатора, специальных ответвителей трафика

5. Формирование отчета потенциально опасных действий в сторону IoT-устройств.

Основываясь на заданных функциях системы контроля взаимодействия в сети, можно выделить основные модули:

- модуль управления списками доверенных устройств;
- модуль управления списками IoT-устройств;
- модуль управления списками потенциально опасных устройств;
- модуль сбора пакетов, который должен реализовать прослушку IoT-устройства, чтобы принять от него потенциально опасный пакет;
- модуль логирования потенциально опасных действий в сети;
- модуль сканирования устройств в сети.

На рисунке 3 цифрами на стрелках обозначены передаваемые данные:

1. IP, MAC адреса устройств IoT и доверенных устройств.
2. IP, MAC адреса доверенных устройств.
3. IP, MAC адреса IoT-устройств.
4. IP, MAC адреса потенциально опасных устройств.

5. IP, MAC адреса потенциально опасных устройств и IP, MAC адреса прослушиваемого IoT-устройства.

6. Время потенциально опасного действия, IP, MAC адреса потенциально опасного устройства, подключенного к сети, либо IP, MAC адреса IoT-устройства и потенциально опасного устройства.

7. IP, MAC адрес IoT-устройства, которое получило пакет и IP, MAC адрес потенциально опасного устройства, с которого этот пакет был отправлен.

Модуль сканирования устройств в сети определяет все подключения в сети.

Модуль управления списками доверенных устройств позволяет заносить устройства в список доверенных.

Модуль управления списками IoT-устройств позволяет заносить устройства в список защищаемых IoT-устройств.

Модуль управления списками потенциально опасных устройств сам определяет, основываясь на работе предыдущих двух модулей, опасно новое подключившееся устройство или нет.

Модуль сбора пакетов получает все пакеты в сети, используя технологии зеркалирования трафика (см. табл. 3).

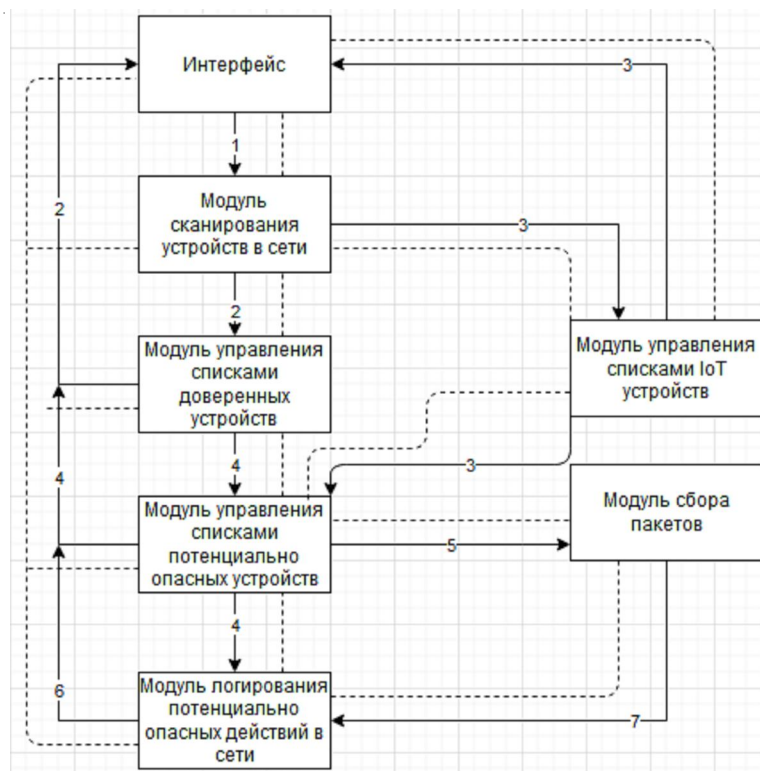


Рис. 3. Система контроля взаимодействия в сети

Модуль логирования потенциально опасных действий в сети формирует информацию о совершенных потенциально опасных действиях (подключение нового, потенциально опасного устройства в сети, передача потенциально опасного пакета устройству IoT), а так же дублирует эту информацию в файлы лога, с указанием времени потенциально опасного действия для повторного анализа.

Таким образом система контроля взаимодействия в сети может обнаружить и пресечь потенциально опасные действия в сторону устройств IoT (посредством блокировки злоумышленника по MAC адресу и др.). Система контроля взаимодействия в сети может использоваться как на предприятии (умные электростанции, торговые и транспортные сети), так и у частных лиц (система умного дома).

Все устройства IoT заведомо содержат уязвимости, так как они находятся не в изолированной системе, а с доступом в интернет. Это подтверждает активный рост вредоносного ПО. Необходимо уделять должное внимание безопасности IoT-устройств. При своевременном анализе сетевого трафика возможно предотвратить угрозу устройству.

СПИСОК ЛИТЕРАТУРЫ

1. Интернет-энциклопедия. – Электрон. текстовые дан. – Режим доступа: <https://ru.wikipedia.org/wiki/> (дата обращения: 14.09.2020). – Загл. с экрана.
2. Лаборатория касперского. – Электрон. текстовые дан. – Режим доступа: <https://www.kaspersky.ru> (дата обращения: 26.09.2020). – Загл. с экрана.
3. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1. – Электрон. текстовые дан. – Режим доступа: <https://www.anti-malware.ru/>

[practice/solutions/iot-the-reference-security-architecture-part-1](https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1) (дата обращения: 14.09.2020). – Загл. с экрана.

4. Gartner представил список стратегических IoT-трендов до 2023 года. – Электрон. текстовые дан. – Режим доступа: <https://iot.ru/promyshlennost/gartner-predstavil-spisok-strategicheskikh-iot-trendov-do-2023-goda> (дата обращения: 26.09.2020). – Загл. с экрана.

5. Juniper Research. IoT Connections to Grow 140% to Hit 50 Billion By 2022, As Edge Computing Accelerates ROI. – Электрон. текстовые дан. – Режим доступа: <https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion> (дата обращения: 12.09.2020). – Загл. с экрана.

REFERENCES

1. *Internet entsiklopediya* [Wikipedia]. URL: <https://ru.wikipedia.org/wiki/> (accessed 14 September 2020).
2. *Laboratoriya Kasperskogo* [Kasperky Lab]. URL: <https://www.kaspersky.ru> (accessed 26 September 2020).
3. *Etalonnaya arkhitektura bezopasnosti interneta veshchey (IoT). Chast 1* [Internet of Things (IoT) Reference Security Architecture. Part 1]. URL: <https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1> (accessed 14 September 2020).
4. *Gartner Has Presented a List of Strategic IoT Trends Until 2023*. URL: <https://iot.ru/promyshlennost/gartner-predstavil-spisok-strategicheskikh-iot-trendov-do-2023-goda> (accessed 26 September 2020).
5. *Juniper Research. IoT Connections to Grow 140% to Hit 50 Billion By 2022, As Edge Computing Accelerates ROI*. URL: <https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion> (accessed 12 September 2020).

NETWORK INTERACTION MONITORING SYSTEM WITH IoT DEVICES CONNECTED

Gleb D. Demyanov

Student, Department of Information Security,
Volgograd State University
005_gleb@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Natalya P. Sadovnikova

Doctor of Sciences (Engineering), Professor,
Department of Computer-Aided Design and Search Engineering,
Volgograd State Technical University
npsn1@yandex.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Abstract. The Internet of Things is a concept of a computer network of physical objects equipped with built-in technologies for interacting with each other or with the external environment, considering the organization of such networks as a phenomenon that can restructure economic and social processes, eliminating the need for human participation from part of actions and operations. IoT technology has had a significant impact on the development of information technology and other industries. According to Forbes, the Internet of Things market is expected to reach \$520 billion in 2021, up from \$235 billion in 2017, indicating a continued growth in demand for such devices in the future. Gartner Research also estimates that the number of devices connected to the Internet will reach 25 billion by 2021, up from 8.4 billion in 2017. Network with IoT devices connected is an indispensable prey for intruders. There are many ways to attack IoT devices. In this article, the authors have identified several methods of protection. Among them, network interaction monitoring through the analysis is highlighted. The paper also describes how to apply this method in practice.

Key words: Internet of Things, IoT devices, network interaction monitoring, information security.



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.3>

УДК 004.056.5

ББК 32.971.35

РАЗРАБОТКА МЕТОДА ПРОВЕДЕНИЯ АУДИТА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Павел Александрович Запороцков

Кандидат физико-математических наук, заместитель начальника отдела эксплуатации информационных систем, технических средств и каналов связи, Управление Росреестра по Волгоградской области
34_upr@rosreestr.ru
ул. Калинина, 4, 400001 г. Волгоград, Российская Федерация

Аннотация. В работе рассмотрены существующие стандарты в области проведения аудита информационной безопасности. Разработана инновационная модель проведения аудита системы защиты информации, базирующаяся на сопоставлении требований мер приказа № 21 ФСТЭК России и способов реализации в подсистемах защиты информации системы защиты персональных данных, даны рекомендации по проверкам конкретных мер защиты и используемым техническим средствам аудита. Разработанный метод апробирован на примере проведения аудита в компании ООО «Лама» выбрано установление соответствия системы защиты персональных данных организации на соответствие требованиям приказа № 21 ФСТЭК России. Разработаны рекомендации по устранению имеющихся недостатков и несоответствий путем переоборудования подсистемы антивирусной защиты и подсистемы межсетевое экранирования и защиты каналов связи.

Ключевые слова: информационная безопасность, аудит системы защиты информации, технические средства аудита, защита каналов связи, антивирусная защита.

Введение

Как известно, принятие решений во всех сферах жизнедеятельности предприятий и организаций базируется на информационных процессах. Анализ таких процессов реализуется на основе информационных моделей, построенных на современных информационно-коммуникационных технологиях.

Информационный ресурс, как часть информационного процесса, является одним из важнейших источников эффективности предприятия вне зависимости от ее сферы деятельности.

Информационные процессы, как и информационные ресурсы управляют информа-

цией различной степени важности для предприятия. В связи с этим защита такой информации представляет одну из важнейших процедур в области обеспечения безопасности государства, значение которой растет с каждым годом.

Проблема защиты информации – надежное обеспечение ее сохранности и установленного статуса использования – является одной из важнейших проблем современности.

В процессе построения систем защиты информации важно понимать, насколько адекватно существующая система защиты информации способна противостоять угрозам информационной безопасности существующим и еще не найденным уязвимостям, а также по-

стоянному процессу изменения в структуре информационного обмена.

Одним из наиболее эффективных способов проверки состояния информационной безопасности на предприятии является аудит.

В соответствии с ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации» под аудитом информационной безопасности понимается систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации [1].

В представленной работе предложен инновационный метод проведения аудита системы технической защиты информации на примере оценки соответствия системы защиты персональных данных ООО «ЛАМА» на соответствие требованиям установленного уровня защищенности.

Предметная область аудита информационной системы технической защиты информации

Аудит проводится на соответствие критериям аудита, которыми являются совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности. Критериями аудита могут быть:

- законодательные нормы и стандарты;
- лучшие практики по обеспечению информационной безопасности;
- внутренние политики информационной безопасности.

Критерии аудита информационной безопасности используются для сопоставления с ними свидетельств аудита информационной безопасности.

По своему типу проведения аудиты подразделяются на внутренние аудиты и внешние аудиты.

Внутренние аудиты (аудиты первой стороны) проводит для внутренних целей сама

организация или от ее имени другая организация. Результаты внутреннего аудита могут служить основанием для декларации о соответствии. Во многих случаях, особенно на малых предприятиях, аудит должен проводиться специалистами (людьми, не несущими ответственности за проверяемую деятельность).

Внешние аудиты включают в себя аудиты, называемые аудиты второй стороны и аудиты третьей стороны. Аудиты второй стороны проводят стороны, заинтересованные в деятельности предприятия, например, потребители или другие лица от их имени. Аудиты третьей стороны проводят внешние независимые организации. Эти организации проводят сертификацию или регистрацию на соответствие требованиям, например, требованиям на соответствие законодательным нормам и федеральным законам, требованиям международных стандартов и т. д.

Национальный стандарт РФ, идентичный международному стандарту, ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента» приводит следующую концепцию проведения аудита [2]:

- организация и проведение аудита;
- подготовка к проведению аудита на месте;
- проведение аудита на месте;
- подготовка и рассылка отчета по аудиту;
- завершение аудита;
- действия по результатам аудита.

Команда аудиторов, обычно состоящая из ведущего аудитора, аудитора, аудитора-стажера, технический эксперт и т. д. перед началом аудита, разрабатывает цели и программу проведения аудита.

Цели могут зависеть от:

- 1) идентифицированных требований информационной безопасности;
- 2) требований нормативных документов;
- 3) уровня качества функционирования проверяемой организации, который отражает случаи возникновения сбоев и инцидентов информационной безопасности и эффективность измерений;
- 4) рисков информационной безопасности организации, подвергающейся аудиту.

Цели аудита можно подразделить на:

- превентивные – направленные на превентивное выявление угроз и уязвимостей и

предотвращение инцидентов информационной безопасности;

– детектирующие – направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты вовремя или после инцидентов информационной безопасности;

– корректирующие – направленные на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов информационной безопасности с учетом вновь выявленных угроз и уязвимостей.

Объем программы аудита может меняться в зависимости от следующих факторов:

1) от масштаба системы информационной безопасности, включающей общее количество сотрудников предприятия и взаимоотношения со сторонними организациями, регулярно работающими на проверяемом предприятии;

2) количество информационных систем предприятия;

3) количество объектов, охваченных системой информационной безопасности:

– сложность системы информационной безопасности (включая количество и критичность процессов и видов деятельности),

– значимость рисков информационной безопасности,

– важность информации и связанных с ней активов,

– сложность информационных систем, сложности использованных информационных технологий;

4) изменение сложности объектов, находящихся в области действия системы информационной безопасности.

По своей форме аудит может быть:

– организационно-нормативным – когда анализируются организационные мероприятия обеспечения информационной безопасности и нормативные акты в данной сфере;

– техническим – когда анализируются технические средства и способы обеспечения информационной безопасности.

Проведение аудита предусматривает следование определенной формальной процедуре проверки объекта. Данная процедура проводится в соответствии с предварительно сформированными формальными описаниями

объекта и процесса аудита, а также актуальных угроз:

– моделью аудита;

– моделью нарушителя / противника;

– моделью угроз;

– общим практическим подходом к проведению аудита;

– общим теоретическим подходом к проведению аудита.

При проведении такой формализации обязательно прописываются следующие аспекты исследования:

– источники угроз;

– защищаемые подсистемы, ресурсы, процессы или другие элементы системы;

– связи между источниками угроз и защищаемыми элементами системы;

– структура и процессы функционирования подсистемы защиты.

Модель аудита включает в себя формализованное описание:

– объекта аудита;

– цели аудита;

– предъявляемых требований;

– используемых практических и теоретических подходов;

– масштаба и глубины;

– исполнителей;

– порядка проведения аудита.

Модель нарушителя / противника включает в себя формализованное описание:

– формализованное понятие нарушителя / противника;

– критерии нарушения информационной безопасности;

– категорирование нарушителей / противников;

– предположения о квалификации, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории нарушителей / злоумышленников;

– предположения о сценариях действий каждой категории нарушителей / злоумышленников;

– уровень полномочий и способы получения доступа к системе для каждой категории нарушителей / злоумышленников.

Описание объекта исследования

В качестве объекта исследования рассматривается ООО «Лама», являющаяся

крупной розничной сетью магазинов по реализации продуктов продовольствия, состоящая из 54 магазинов формата универсам, супермаркет, гипермаркет и центрального офиса. Оперативное управление ООО «Лама» осуществляется генеральным директором в соответствии с уставом. Функции обеспечения защиты информации возложены на специалиста по информационной безопасности, входящего в отдел АСУ. Виды обрабатываемой информации: – персональные данные (далее – ПДн) сотрудников и физических лиц, не являющихся сотрудниками и коммерческая тайна. Примерный объем обрабатываемых персональных данных – более 100 000. Обработка персональных данных происходит как с использованием средств автоматизации (в информационных системах персональных данных), так и без использования средств автоматизации (на документальных носителях).

В ООО «Лама» персональные данные обрабатываются в следующих информационных системах персональных данных (далее – ИСПДн):

- 1С: Бухгалтерия;
- 1С: Бухгалтерия;
- 1С: Управление продажами.

Предоставление сервисов информационных систем персональных данных пользователям реализуется посредством локальной вычислительной сети. Сетевая архитектура локальной вычислительной сети построена на базе оборудования Dlink (см. рис. 1).

Ядром сети выступает маршрутизатор DSR-1000. За коммутацию серверного оборудования отвечает коммутатор типа DGS-1008MP. За коммутацию рабочих станций отвечают коммутаторы серии DES-1050G.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 [3] определяются 4 уровня защищенности, в соответствии с которыми обеспечивается защита персональных данных. Уровень защищенности определяется категорией обрабатываемой информации, типом актуальных угроз и числом субъектов ПДн.

Для всех ИСПДн ООО «Лама» характерны угрозы 3-го типа, не связанные с наличием недеklarированных возможностей, так как все применяемое программное обеспечение лицензировано и имеет разрешение к применению

на территории Российской Федерации. Так как ООО «Лама» не обрабатывают специальные, биометрические и общедоступные ПДн, можно установить, что ИСПДн ООО «Лама» обрабатывают иные категории ПДн.

На основании вышеизложенной информации и Постановления Правительства РФ от 1 ноября 2012 г. № 1119, уровень защищенности устанавливается как УЗ-4 [3].

На основании сведений о уровне защищенности можно установить содержание мер по обеспечению безопасности ПДн в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [4]:

- идентификация и аутентификация: ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6;
- управление доступом: УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.13, УПД.14, УПД.15, УПД.16;
- регистрация событий безопасности: РСБ.1, РСБ.2, РСБ.3, РСБ.7;
- антивирусная защита: АВЗ.1, АВЗ.2;
- анализ защищенности: АНЗ.2;
- защита технических средств: ЗТС.3, ЗТС.4;
- защита информационных систем: ЗИС.3.

Сведения о необходимости соответствия техническим мерам по защите персональных данных в этом случае будут являться критериями аудита.

3. Разработка методики аудита

В качестве системы технической защиты информации ООО «Лама» рассматривается система защиты персональных данных ООО «Лама» (далее – СЗПДн). СЗПДн предназначена для соблюдения требований Федерального закона № 152-ФЗ «О персональных данных» [5], требований нормативных документов и позволяет минимизировать правовые и репутационные риски, связанные с потенциальными утечками персональных данных и несоблюдением законодательства Российской Федерации.

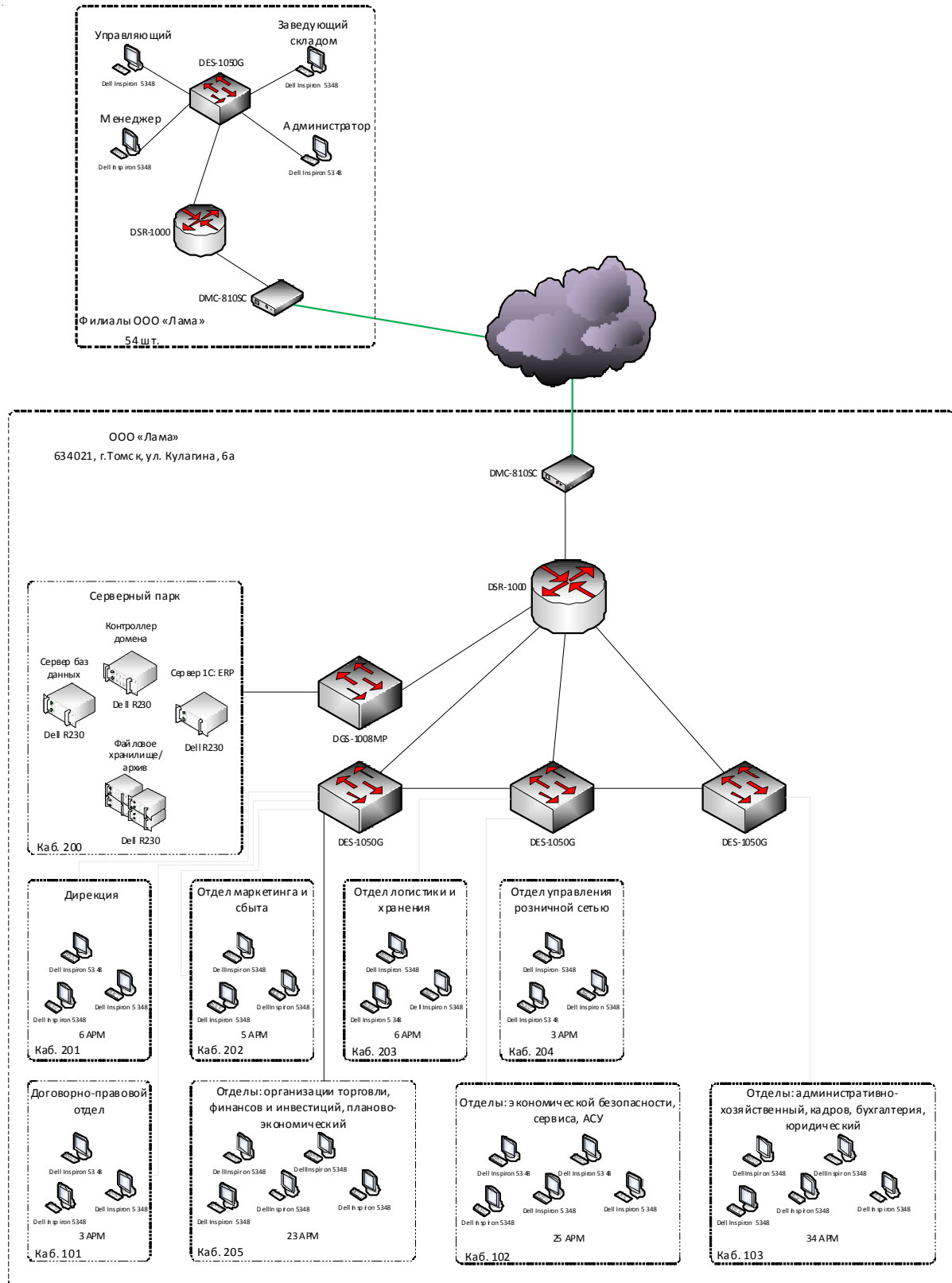


Рис. 1. Структура локальной вычислительной сети ООО «Лама»

В соответствии с минимально необходимым комплексом мер в состав типовой СЗПДн входят следующие подсистемы:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема антивирусной защиты;
- подсистема межсетевое экранирование и защиты каналов связи;
- подсистема управления системой защиты персональных данных.

Для проверки корректности применяемых мер по защите информации ООО «Лама» прибегает к внутреннему аудиту СЗПДн.

Аудит СЗПДн проводится силами отдела АСУ ООО «Лама» и включает в себя следующие этапы:

- планирование аудита;
- подготовка аудита;
- проведение аудита;
- составление отчетной документации по результатам аудита.

Целью планирования аудита является обеспечение проведения проверки наилучшим (оптимальным) образом. Результаты процесса планирования оформляются в двух документах: плане аудита и программе аудита.

В плане аудита отмечается объект аудита, организационная единица, место проведения аудита, критерии аудита, сведения об аудиторах и периодах проведения аудита.

Аудит начинается с вводного совещания, которое проводит руководитель аудита в срок, указанный в программе аудита или в другое согласованное сторонами время.

Во время аудита информация, относящаяся к целям аудита, области и критериям аудита, включая информацию, касающуюся взаимодействия между подразделениями, деятельности и процессов, должна быть собрана путем необходимых выборок и обработана. Свидетельством аудита может быть только информация, которая может быть обработана. Свидетельства аудита должны быть зарегистрированы.

Источниками исходной информации для аудиторов в ходе проверки являются: документы, регламентирующие деятельность подразделения и процессы, процедуры, методики, приказы, планы, регистрационные журналы, протоколы совещаний.

При сборе свидетельств аудита необходимо использовать следующие методы:

- опросы;
- наблюдение за деятельностью;
- техническая проверка;
- оценивание.

Программа проведения аудита является частным случаем общего алгоритма проведения аудита и детализирует перечень аудиторских процедур подлежащих проведению. Программа служит подробной инструкцией для аудиторской команды и одновременно средством контроля для руководства компании.

Программа проведения аудита реализуется путем поэтапной проверки соответствующих подсистем СЗПДн и мер, предназначенных для реализации требований по защите информации, предъявляемых к этим подсистемам. На рисунке 2 представлена методика проведения аудита СЗПДн.

Для каждой из подсистем СЗПДн (УПД.1, УПД.3...ИАФ.1 и т. д.) используется своя методика проверки реализации мер информационной безопасности.

Технические средства аудита

Для аудита информационной безопасности СЗПДн могут применяться различные технические средства.

Для аудита подсистем управления доступом, регистрации и учета, обеспечения целостности может применяться система анализа защищенности Сканер-ВС.

Сканер-ВС – система комплексного анализа защищенности, позволяющая обеспечить своевременное выявление уязвимостей в ИТ-инфраструктуре организаций любого масштаба. С помощью Сканер-ВС можно проводить тестирование на проникновение, сканирование уязвимостей, а также анализ конфигурации, организовать непрерывный контроль защищенности. В качестве средства аудита СЗПДн Сканер-ВС дает широкий функционал по реализации мер сетевого и локального аудита-контроль появления новых сетевых узлов и сервисов, идентификация ОС и приложений, трассировка маршрутов передачи данных, построение топологии сети организации.

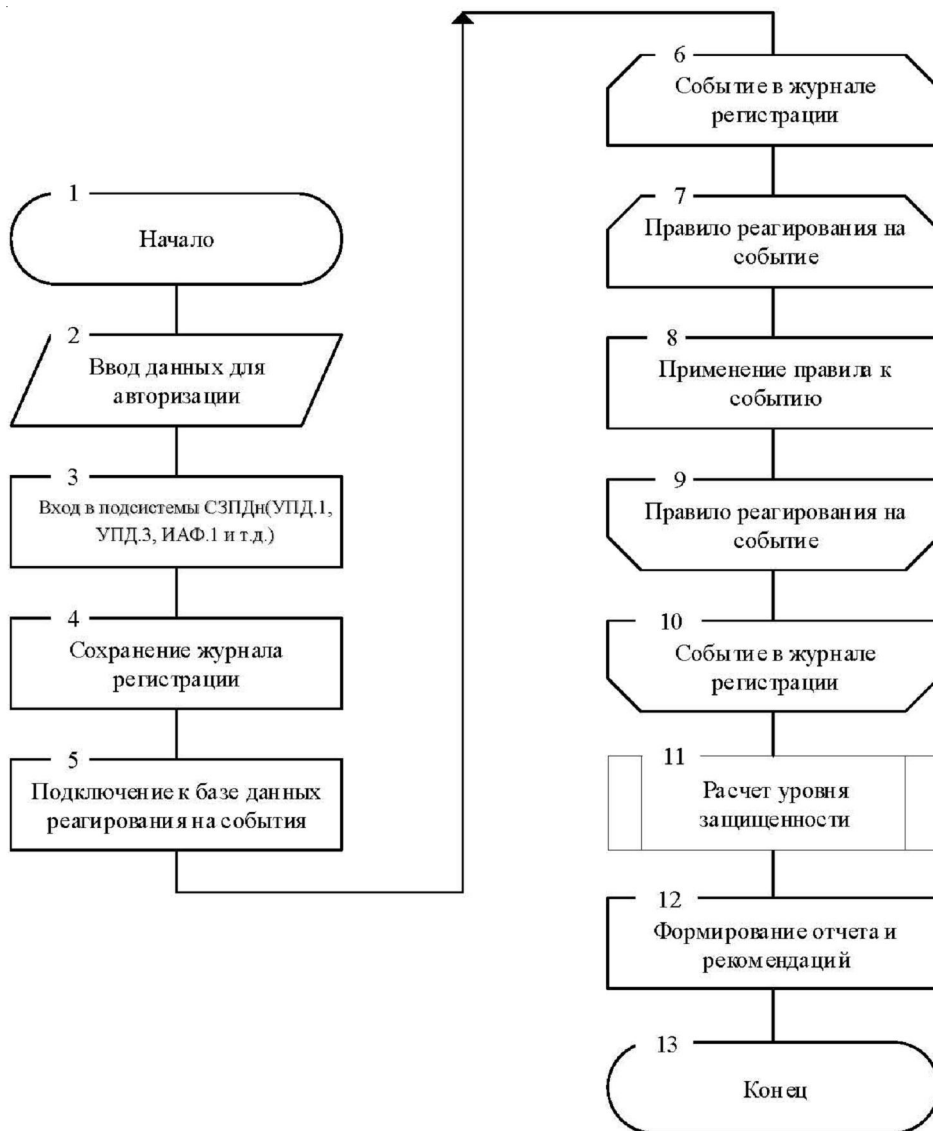


Рис. 2. Методика проведения аудита СЗПДн

Сканер-ВС позволяет проводить аудит установленного аппаратного и программного обеспечения – инвентаризацию программных и аппаратных средств локальной системы, включая параметры установленных операционных систем, программное обеспечение, информацию о пользователях системы, историю подключений к беспроводным сетям, данные системных, коммуникационных и периферийных устройств (центральный процессор, материнская плата, мост, оперативная память и др.), в том числе носителей информации и USB-устройств. Функция сравнения отчетов позволяет отслеживать изменения конфигурации системы. Для аудита мер ИАФ.2, УПД.3, УПД.4, УПД.6 используется

средство локального аудита паролей Сканер-ВС, предназначенное для поиска и выявления на локальной рабочей станции неустойчивых к взлому паролей.

Для аудита мер УПД.14 применяется средство аудита беспроводных сетей. Средство аудита беспроводных сетей предназначено для обнаружения, сканирования и проведения пассивных и активных атак на подбор паролей в беспроводных сетях с WEP, WPA и WPA-2 шифрованием.

Модуль сетевого анализа предназначен для перехвата, анализа и фильтрации сетевого трафика.

Для поиска потенциальных уязвимостей в сети используется модуль «Поиск уязвимос-

тей». Под уязвимостью ПО подразумевается дефект, который может стать причиной нарушения информационной безопасности.

В качестве средства аудита мер ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.4, УПД.5, УПД.6 может также использоваться программное средство ChangeAuditor 5.0.

ChangeAuditor 5.0 – является инструментом для оперативного аудита изменений в реальном масштабе времени на серверах служб каталогов, Exchange, а также на файловых серверах под управлением операционной системы Windows. Кроме аудита, в ChangeAuditor 5.0 можно блокировать изменения. Например, запретить добавление в группу AD новых пользователей или запретить изменение файла / папки.

В качестве средства аудита мер РСБ.2, РСБ.3, РСБ.7 может также использоваться менеджмент логов QuestInTrust – интеллектуальный, масштабируемый инструмент управления журналом событий, который позволяет отслеживать все действия пользователей на рабочих станциях и администраторах от входа в систему до выхода из системы и всего того, что было между этими событиями. После сбора вся статистика (события) приводится к состоянию вида: когда произошло, что произошло, где произошло, кто выполнил действие, откуда это действие было выполнено. InTrust может обрабатывать до 60 000 событий в секунду из 10 000 источников. Часто подобные агенты-сборщики устанавливаются на рабочие станции, чтобы отслеживать события WindowseventlogSysmon (отслеживания изменений значений реестра, создания новых процессов с неправильных хэшем и других), логов PowerShell.

В соответствии со сведениями об объекте исследования и методикой проведения аудита была проведена аналитическая реализация программы аудита СЗПДн ООО «Лама».

По результатам аудита установлены 19 соответствий и 7 несоответствий. Были выданы рекомендации на разработку 7 корректирующих действий для успешного прохождения аудита, в частности:

– разработать план корректирующих действий, определить ответственных лиц и сроки исполнения;

– произвести замену средства антивирусной защиты на средство, соответствующее требованиям ФСТЭК России по информационной безопасности, произвести его настройку и обновление базы сигнатур до актуальной версии;

– произвести выбор средства, закупку и пуско-наладку средства межсетевое экранирования и шифрования в соответствии с требованиями руководящих документов ФСТЭК и ФСБ России;

– произвести повторный аудит по выявленным несоответствиям и определить корректность их устранения.

Заключение

Были рассмотрены существующие стандарты в области проведения аудита информационной безопасности. Дано описание объекта исследования – компания ООО «Лама». В качестве критериев аудита выбрано установление соответствия системы защиты персональных данных ООО «Лама» на соответствие требованиям приказа № 21 ФСТЭК России.

Разработана модель проведения аудита системы защиты информации, базирующаяся на сопоставлении требований мер приказа № 21 ФСТЭК России и способов реализации в подсистемах защиты информации системы защиты персональных данных, даны рекомендации по проверкам конкретных мер защиты и используемым техническим средствам аудита.

Проведен аналитический аудит системы защиты персональных данных ООО «Лама», по результатам аудита установлено 19 соответствий и 7 несоответствий, в качестве рекомендаций по повышению уровня защищенности рекомендуется переоборудование подсистемы антивирусной защиты и подсистемы межсетевое экранирования и защиты каналов связи.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в

организации. – Электрон. текстовые дан. – Режим доступа: <https://internet-law.ru/gosts/gost/48411>. – Загл. с экрана.

2. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента. – Электрон. текстовые дан. – Режим доступа: <https://internet-law.ru/gosts/gost/52229>. – Загл. с экрана.

3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных». – Доступ из справ.-правовой системы «КонсультантПлюс».

REFERENCES

1. *GOST R 53114-2008 Nacional'nyj standart Rossijskoj Federacii. Zashchita informacii. Obespechenie informacionnoj bezopasnosti v organizacii* [The National Standard of the Russian Federation. Information Security. Ensuring Information

Security in the Organization]. URL: <https://internet-law.ru/gosts/gost/48411>.

2. *GOST R ISO 19011-2012. Rukovodyashchie ukazaniya po auditu sistem menedzhmenta* [Guidelines for the Audit of Management Systems]. URL: <https://internet-law.ru/gosts/gost/52229>.

3. *Postanovlenie Pravitel'stva RF ot 1 noyabrya 2012 g. № 1119 «Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh»* [Resolution of the Government of the Russian Federation of 8 November, 2012 no. 647 “On Approval of the Requirements for the Protection of Personal Data During Their Processing in Personal Data Information Systems”]. Access from Reference Legal System “KonsultantPlyus”.

4. *Prikaz FSTEK Rossii ot 18 fevralya 2013 g. № 21 «Ob utverzhdenii sostava i sodержaniya organizacionnyh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh»* [Order FSTEK of 18 February 2013 no. 21 “On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data During Their Processing in Personal Data Information Systems”]. Access from Reference Legal System “KonsultantPlyus”.

5. *Federal'nyj zakon ot 27.07.2006 № 152-FZ (red. ot 21.07.2014) «O personal'nyh dannyh»* [Federal Law of 27 July 2006 no. 152-FZ (as Amended on 21 July 2014) “About Personal Data”]. Access from Reference Legal System “KonsultantPlyus”.

DEVELOPMENT OF A METHOD FOR CONDUCTING AN AUDIT OF THE INFORMATION SECURITY SYSTEM

Pavel A. Zaporotkov

Candidate of Sciences (Physics and Mathematics), Deputy Head of the Department of Operation of Information Systems, Technical Means and Communication Channels, Department of Rosreestr for Volgograd Region
34_upr@rosreestr.ru
Kalinina St, 4, 400001 Volgograd, Russian Federation

Abstract. Information processes, as well as information resources, manage information of varying degrees of importance for the enterprise. In this regard, the protection of such information is one of the most important procedures in the field of state security, the importance of which is growing every year. The problem of information security – the reliable provision of its safety and the established status of use – is one of the most important problems of our time. The paper considers the existing standards in the field of information security audit. The author has developed an innovative model of audit of the information security system based on the comparison of demand measures of order no. 21 of the FSTEK of Russia and ways of implementation in the subsystem of the information system of personal data protection, the

recommendations for inspections of specific measures of protection and used technology audit technical means. The developed method is tested on the example of conducting an audit in “Lama” LLC company. The choice was made to establish the compliance of the organization’s personal data protection system with the requirements of order no. 21 of the FSTEC of Russia. Recommendations have been developed to eliminate the existing shortcomings and inconsistencies by re-equipping the anti-virus protection subsystem and the subsystem of inter-network shielding and protection of communication channels.

Key words: information security, audit of the information security system, technical means of audit, protection of communication channels, anti-virus protection.



www.volsu.ru

ИННОВАЦИИ В МЕТАЛЛУРГИИ И МАТЕРИАЛОВЕДЕНИИ

DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.4>

УДК 539.2:537.531

ББК 22.37

INVESTIGATION OF THE PHYSICAL AND MECHANICAL PROPERTIES OF RADIO-ABSORBING MATERIALS

Alexander V. Vasiliev

Doctor of Sciences (Engineering), Professor, Department of Heat Engineering and Hydraulics,
Volgograd State Technical University
vasilyev@vstu.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Anatoly M. Afanasiev

Doctor of Sciences (Engineering), Professor, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The paper studies the physical and mechanical properties of radio-absorbing materials. It is shown that to ensure an effective level of material absorption, it is necessary to introduce carbon fibers in the amount of at least 0.25% by weight.

Key words: electromagnetic radiation, radio-absorbing materials, physical and mechanical properties, carbon fibers, plasticizer.

Currently, there is a need to manufacture radio-absorbing materials for the manufacture of clothing and covers for technical purposes to protect against electromagnetic radiation. Such materials should be light and elastic and should not cause discomfort when in contact with a person. Previously, film radio-absorbing materials were actively developed to ensure the above conditions [5]. High-capacity polymers are of

particular interest for the production of such materials. A significant number of different polymers are known, but plasticized polyvinyl chloride (PVC) has found wide industrial application [6; 8].

Plasticized polyvinyl chloride processing technologies make it possible to obtain films with different degrees of rigidity: hard, soft, and ultra-soft. The content of the plasticizer in it varies from

20 to 60 weight parts. It is obvious that the amount of plasticizer affects the properties of PVC films, and an increase in the content of plasticizer leads to an increase in the quality of mixing the components of plastisol.

In addition to PVC and plasticizers, plastisol also contains a filler, stabilizer and lubricant (stearic acid, calcium stearate, etc.). However, these components have little effect on the technological properties of the PVC paste, such as viscosity and fluidity. The study of the effect of the plasticizer content on the radiophysical properties of film materials based on polyvinyl chloride is of practical importance [1; 2; 3; 4; 7].

In order to obtain polyvinyl chloride films and evaluate the effect of the plasticizer on radio absorption, films with different plasticizer content were obtained. The basis was a standard recipe based on PVC (see Table), which is often used by the domestic industry to produce polymer films. The amount of DOP was from 60 to 90 wt. h. per 100 wt. h. PVC in increments of 10 wt. h. At the same time, the DOS content remained unchanged – 10 wt. h. per 100 weight parts of PVC.

All films had a smooth and flat surface without pronounced defects and irregularities.

In connection with the field of application of radio-absorbing polymer materials, it can be argued that in addition to their radiophysical properties, their physical and mechanical properties are of great importance. The materials can be used for the manufacture of products of complex shapes, while they have sufficiently high performance characteristics, especially strength and elasticity.

In this paper, we investigated the effect of an electrically conductive filler on the tensile strength and elongation at break of monolithic and porous films based on polyvinyl chloride modified with carbon fiber.

The analysis of the data showed that the filled monolithic and porous films are characterized by a

general tendency to reduce the elongation and strength when introducing carbon fibers. It should be noted that the samples cut in the direction of the squeegee movement have higher physical and mechanical properties. This is because the carbon fibers are mostly aligned along the doctor's motion, and their atoms are combined into microscopic crystals that are aligned parallel to each other, giving the fiber a higher tensile strength.

From the diagrams (see fig. 1–4), it can be seen that, in comparison with unfilled monolithic films, a noticeable decrease in these properties of filled films is achieved with a low content of carbon fiber – 0.25 wt.h. per 100 weight parts of PVC. A further increase in the degree of filling of the films with carbon fiber to 0.75% by weight practically does not affect the decrease in strength properties. If the filling level exceeds 0.75 wt. h., there is a secondary decrease in the physical and mechanical properties.

The decrease in elongation at the break of the filled films is associated with the sorption of the plasticizer by carbon fiber and a decrease in its content in the polymer matrix. With an increase in the content of carbon fibers, the proportion of the adsorbed plasticizer increases, the stiffness of the polymer matrix increases, and the elongation at break decreases, which is confirmed by experimental results. However, the increase in stiffness should be accompanied by an increase in strength, which, according to experimental data, monotonically decreases. The explanation of this effect is associated with the formula.

Technologies of processing of PVC plastisols allow to receive films with various degrees of rigidity: rigid, soft, ultra-soft. The content of the plasticizer in it varies from 40 to 100 weight parts. At 100 wt.h. of PVC, it is obvious that the amount of plasticizer affects the properties of PVC films, and an increase in the content of plasticizer leads to an increase in the quality of mixing the components of plastisol.

Recipe for obtaining a film based on polyvinyl chloride

Component Name	Bulk parts per 100 wt. h. PVC
PVC-E	100
DOF	60-70-80-90
DOS	10
StCa	1,5
CH ₃ (CH ₂) ₁₆ COOH	2

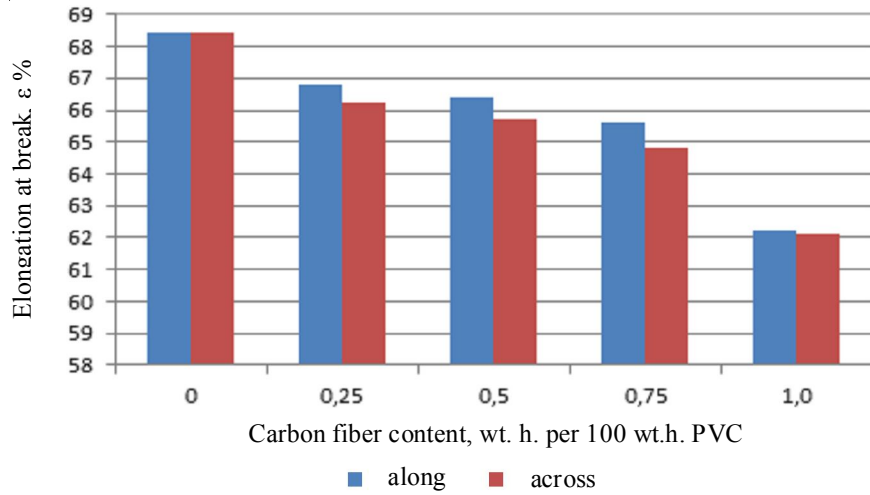


Fig. 1. Diagram of elongation at break of monolithic PVC-based films filled with carbon fiber

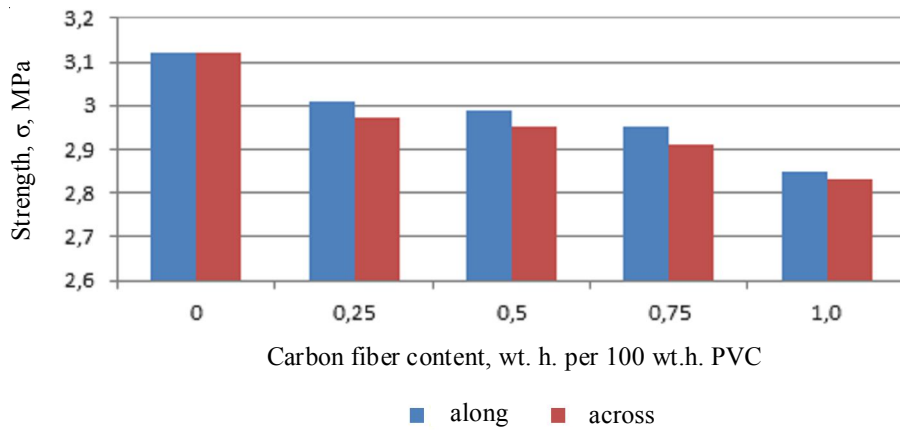


Fig. 2. Diagram of the tensile strength of monolithic PVC-based films filled with carbon fiber

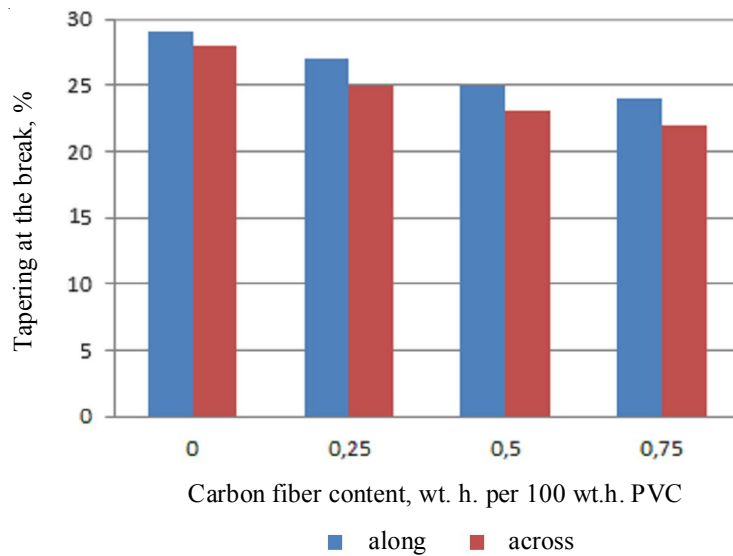


Fig. 3. Diagram of elongation at break of porous PVC-based films filled with carbon fiber

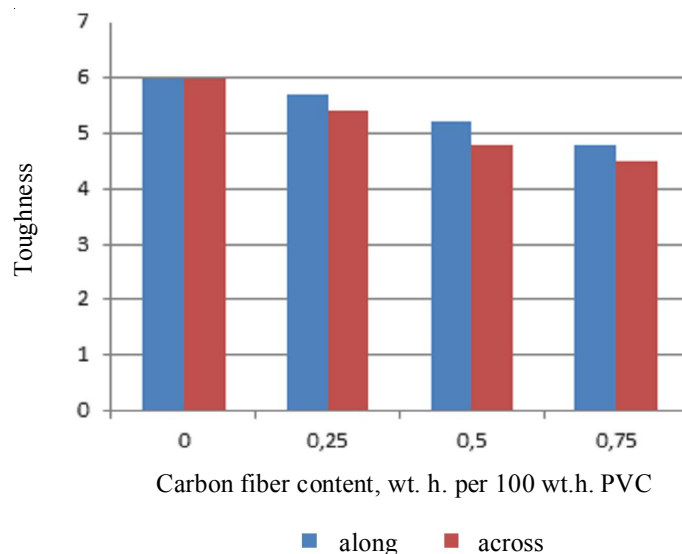


Fig. 4. Diagram of the tensile strength of porous PVC-based films filled with carbon fiber

In order to obtain polyvinyl chloride films and evaluate the effect of the plasticizer on radio absorption, films with different plasticizer content were obtained. The basis was a standard recipe based on PVC, which is often used in the domestic industry for the production of polymer films. The amount of DOP was from 60 to 90 wt. h. per 100 wt. h. PVC in increments of 10 wt. h. At the same time, the DOS content remained unchanged – 10 wt. h. per 100 weight parts of PVC.

When testing the technology for manufacturing plastisols and films, it was found that the introduction of carbon fibers in an amount of less than 0.25% by weight did not provide an effective level of absorption of the material. For the production of monolithic films with an increase in the filler content of more than 1.5% by weight. From the organoleptic point of view, the films became rigid and had obvious defects-alternating transparent areas and areas of crumpled filler. In the case of porous films, the increase in the carbon fiber content did not affect the technological parameters of plastisol, the film was formed evenly. The introduction of a filler with more than 1.25 wt.h. is not recommended, this leads to a significant decrease in the efficiency of the absorption of the material by electromagnetic radiation.

Thus, the amount of imported carbon fiber was in the range of 0.25 to 1.5 weight parts. per 100 weight parts of polyvinyl chloride for monolithic films and from 0.25 to 1.25 weight parts per 100 weight parts of PVC for porous films, the division is 0.25.

REFERENCES

1. Belonenko M.B. Vliyanie peremennogo jelektricheskogo polja na provodimost' odnoslojnyh uglerodnyh nanotrubok poluprovodnikovogo tipa. *Fizika i tehnika poluprovodnikov*, 2010, no. 44, pp. 1248-1253.
2. Boroznin S.V., Zaporockova I.V., Boroznina E.V. Kapilljarnye jeffekty v borouglerodnyh nanotrubkah. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost [Science Journal of Volgograd State University. Innovation Activity]*, 2013, no. 8, pp. 38-43.
3. Elbakyan L.S. The Polymers Filled Eith Carbon Nanotubes as New Materials in Stomatology. *European Polymer Congress*, 2013, pp. 30-31.
4. Khokhlov V.M. Wear Laws at Elastic Interaction. *Russia Engineering Research*, 1996, no. 16, pp. 11-12.
5. Kim J.S. Improved Electrical Conductivity of Very Long Multi-Walled Carbon Nanotube Bundle/ Poly (Methyl Methacrylate) Composites. *Carbon*, 2011, no. 49, pp. 2127-2133.
6. Semaan Ch. Influence of Wrapping on Some Properties of MWCNT-PMMA and MWCNT-PE Composites. *Polymer Bulletin*, 2013, no. 70, pp. 1919-1936.
7. Semenova L.M., et al. Laws of Formation of Diffusion Layers and Solution of the Diffusion Problem in Temperature-Cycle Carbonitriding of Steel. *Metal Science and Heat Treatment*, 2013, no. 55, pp. 34-37.
8. Zaporotskova I.V. About Adsorption of the Polyethylene Monomer Unit on the Single-Walled Carbon Nanotubes Surface, European Polymer Congress. *Book of Abstracts Pisa*, 2013, pp. 3-6.

ИССЛЕДОВАНИЕ ФИЗИКО-МЕХАНИЧЕСКИХ СВОЙСТВ РАДИОПОГЛОЩАЮЩИХ МАТЕРИАЛОВ

Александр Викторович Васильев

Доктор технических наук, профессор кафедры теплотехники и гидравлики,
Волгоградский государственный технический университет
vasilyev@vstu.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Анатолий Михайлович Афанасьев

Доктор технических наук, профессор кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе исследуются физико-механические свойства радиопоглощающих материалов. Показано, что для обеспечения эффективного уровня поглощения материала необходимо введение углеродных волокон в количестве не менее 0,25 % по массе.

Ключевые слова: электромагнитное излучение, радиопоглощающие материалы, физико-механические свойства, углеродные волокна, пластификатор.



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.5>

УДК 544.2

ББК 24.5

ИССЛЕДОВАНИЕ ВЗАИМОДЕЙСТВИЯ УГЛЕКИСЛОГО ГАЗА С МОДИФИЦИРОВАННЫМИ ФУНКЦИОНАЛЬНЫМИ ГРУППАМИ НАНОТРУБОК ¹

Лев Васильевич Кожитов

Доктор технических наук, профессор кафедры технологии материалов электроники,
Национальный исследовательский технологический университет «МИСиС»
kozitov@misis.ru
просп. Ленинский, 4, 119049 г. Москва, Российская Федерация

Ирина Владимировна Запороцкова

Доктор физико-математических наук, профессор,
Директор Института приоритетных технологий,
Волгоградский государственный университет
sefm@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Наталья Павловна Борознина

Доктор физико-математических наук,
профессор кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
boroznina.natalya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Сергей Владимирович Борознин

Кандидат физико-математических наук,
доцент кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
boroznin@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владимир Витальевич Акатьев

Старший преподаватель,
доцент кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
sefm@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В представленной статье проводится теоретическое исследование возможности взаимодействия одного из распространенных веществ в природе – углекислого газа – с модифицированными функциональными карбоксильной и аминной группами углеродной нанотрубки и бороуглеродной нанотрубки типа ВС5. В статье проанализированы результаты взаимодействия и проведен сравнительный анализ эффективности сорбционного взаимодействия наносистемы с молекулой углекислого газа. Даны рекомендации дальнейшего использования результатов в качестве основы для создания высокочувствительного сенсорного устройства нового поколения для выявления микроколичеств веществ.

Ключевые слова: нанотрубки, сенсорные устройства, молекула углекислого газа, сорбционное взаимодействие, модификация.

Введение

Одной из современных проблем развития технологий является проблема энергосбережения и энергоэффективности новых производств и используемого оборудования. Как правило, высокотехнологичное оборудование потребляет большое количество электроэнергии, что ведет к различным ресурсным затратам. В числе таких важных устройств присутствуют и одни из наиболее востребованных в настоящее время сенсорные устройства различного типа, которые используются для обнаружения и идентификации веществ в различных средах. Они могут применяться для обеспечения экологического мониторинга, для контроля загрязненности воды и воздуха, определение источников промышленных выбросов и для других целей.

Одной из подобных и важных областей применения сенсорных устройств – это область контроля загрязнения воздуха в помещениях. Помимо жилых и производственных помещений особенно актуальным будет являться контроль и поддержание чистоты воздуха в медицинских учреждениях, палатах интенсивной терапии, боксах для новорожденных, а также для поддержания условий в лабораториях для проведения исследований. В настоящее время для выполнения названных задач во всех областях используется довольно энергозатратное оборудование (различные газоанализаторы, спектральные приборы и т. п.). Поэтому необходим поиск новых решений и создание новых недорогих универсальных сенсорных устройств, энергоэффективность которых

будет обеспечиваться применением принципиально новых материалов, в том числе, в качестве сенсорных датчиков.

Исследования, посвященные использованию углеродных нанотрубок (УНТ) в качестве датчика для определения различных газов, достаточно обширны [4; 5; 6; 7; 9; 10]. Однако ещё не была рассмотрена возможность использования гранично-модифицированных функциональными группами УНТ для идентификации молекул газов.

Ранее были проведены исследования, посвященные сорбционному и сенсорному взаимодействию модифицированных наноструктур на основе углерода в отношении атомов и ионов щелочных металлов [1; 2; 3; 11]. Эти исследования доказали наличие высокой чувствительности наносистем к микроколичествам веществ. Они могут создавать предпосылки к расширению типов детектирующих систем и видов определяемых веществ. Подобные теоретические исследования ранее не выполнялись, что определяет актуальность материала, представленного в статье.

Результаты и обсуждение

Проведенные ранее исследования, посвященные граничному модифицированию углеродной нанотрубки аминной группой, показали образование стабильного химического комплекса [8]. Для изучения сорбционного взаимодействия молекулы углекислого газа с комплексом «углеродная нанотрубка – аминная группа» было выполнено моделирование процесса присоединения путем пошагового приближения исследуемой молекулы к крае-

вого атому функциональной группы (рис. 1). По результатам исследования были построены кривые, показывающие общую картину взаимодействия (рис. 2). Анализ результатов показал, что присоединение молекулы происходит безбарьерно. Установленное расстояние взаимодействия 2 Å и энергия взаимодействия 1,59 eV доказывает наличие слабого ван-дерваальсового взаимодействия. Такой тип взаимодействия обеспечит возможность многократного использования подобного сенсорного устройства без его разрушения или изменения его свойств, что могло бы произойти в случае образования химической связи между наносистемой и исследуемым веществом.

Заключение

Несмотря на высокую популярность исследований в области сенсорных свойств нанотрубок, ранее не было приведено теоретических обоснований, подтвержденных компьютерными расчетами электронно-энергетичес-

ких характеристик сорбционной и сенсорной активности нанотрубчатых материалов, включающих компьютерное моделирование взаимодействия между модифицированной углеродной нанотрубкой и молекулами газов (в том числе углекислого газа). Также стоящая довольно остро проблема оценки качества воздуха и помещениях, позволяет судить об актуальности данных исследований.

Выполненные исследования доказывают реализацию слабого физического сорбционного взаимодействия между наносистемой, состоящей из углеродной нанотрубки, гранично-модифицированной аминной группой, и молекулой углекислого газа. Это позволяет говорить о возможном сенсорном взаимодействии, которое позволит использовать подобный комплекс для обнаружения микроколичества вещества – углекислого газа. На основе этого можно сделать вывод, что модифицированные углеродные нанотрубки могут являться элементами датчиков для определения качества воздуха в помещении, выступать в качестве

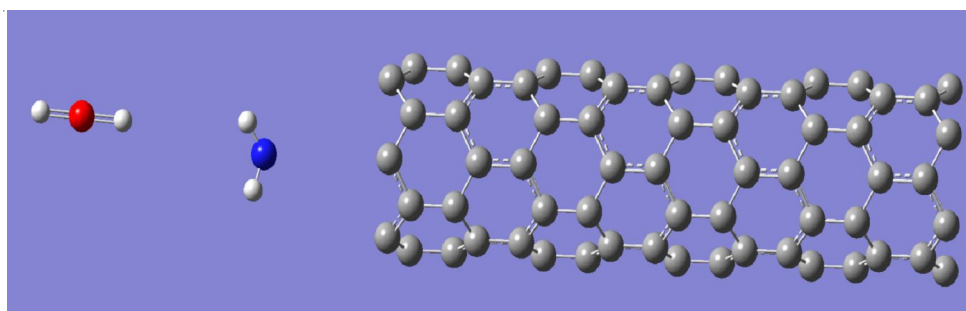


Рис. 1. Модель модифицированной аминной группой углеродной нанотрубки при взаимодействии с молекулой углекислого газа

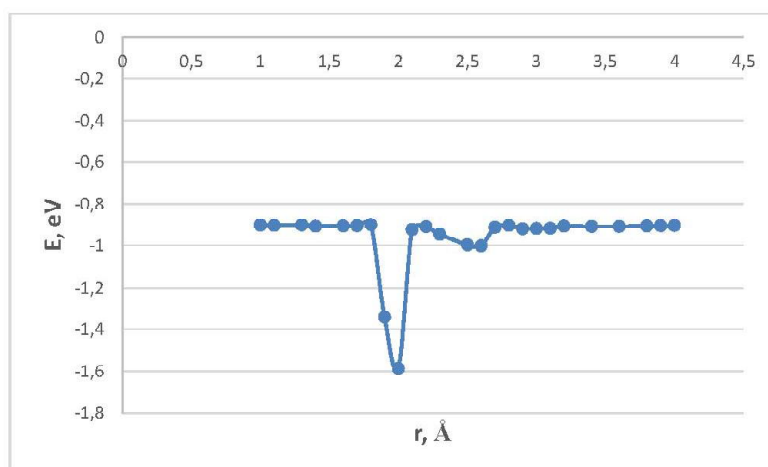


Рис. 2. Энергетическая кривая взаимодействия системы УНТ-аминная группа с молекулой CO₂

зондов кантиливеров атомно-силовых микроскопов и других устройств.

ПРИМЕЧАНИЕ

¹ Исследование выполнено при финансовой поддержке гранта Президента РФ и стипендии президента РФ № МК-1758.2020.8 № СП-798.2019.1.

The reported study was funded by the grant of the President of the Russian Federation and the scholarship of the President of the Russian Federation no. МК-1758.2020.8 no. SP-798.2019.1.

СПИСОК ЛИТЕРАТУРЫ

1. Boroznina, N. P. Comparative Analysis of Sensor Activity of Carbon Nanotubes Modified with Functional Groups / N. P. Boroznina, I. V. Zaporotskova, S. V. Boroznin // *Journal of Nano- and Electronic Physics*. – 2017. – Vol. 9, № 3. – Art. 03046.
2. Boroznina, N. P. Modeling the Sensing Activity of Carbon Nanotubes Functionalized with the Carboxyl, Amino, or Nitro Group Toward Alkali Metals / N. P. Boroznina, I. V. Zaporotskova // *Russian Microelectronics*. – 2017. – Vol. 46, № 8. – P. 580–584.
3. Boroznina, N. P. Sensitivity of Carboxyl-Modified Carbon Nanotubes to Alkaline Metals / N. P. Boroznina, I. V. Zaporotskova, S. V. Boroznin // *Nanosystems: Physic, Chemistry, Mathematics*. – 2018. – Vol. 9 (1). – P. 79–84.
4. Highly Sensitive and Selective Carbon Nanotube-Based Gas Sensor Arrays Functionalized with Different Metallic Nanoparticles / A. Abdelhalim [et al.] // *Sens. Actuators B Chem.* – 2015. – Vol. 220. – P. 1288–1296.
5. Hydrogen Sensors Based on Aligned Carbon Nanotubes in an Anodic Aluminum Oxide Template with Palladium as a Top Electrode / D. Ding [et al.] // *Sens. Actuators B Chem.* – 2007. – Vol. 124, № 1. – P. 12–17.
6. Metal-Modified and Vertically Aligned Carbon Nanotube Sensors Array for Landfill Gas Monitoring Applications / M. Penza [et al.]. – *Nanotechnology*. – 2010. – Vol. 21, № 10. – Art. 105501.
7. Room-Temperature, Selective Detection of Benzene at Trace Levels Using Plasma-Treated Metal-Decorated Multiwalled Carbon Nanotubes / R. Leghrib // *Carbon*. – 2010. – Vol. 48, № 12. – P. 3477–3484.
8. Sensors Based on Amino Group Surface-Modified CNTs / N. P. Boroznina [et al.] // *Chemosensors*. – 2019. – Vol. 7. – P. 1–7.
9. Three-Terminal CNTS Gas Sensor for N₂ Detection / C. Huang [et al.] // *Diam. Relat. Mater.* – 2005. – Vol. 14, № 11–12. – P. 1872–1875.
10. Understanding the Sensor Response of Metal-Decorated Carbon Nanotubes / D. R. Kauffman [et al.] // *Nano Lett.* – 2010. – Vol. 10. – P. 958–963.

11. Zaporotskova, I. V. Sensor Activity with Respect to Alkali Metals of a Carbon Nanotube Edge-Modified with Amino Group / I. V. Zaporotskova, L. V. Kozhitov, N. P. Boroznina // *Russ. J. Inorg. Chem.* – 2017. – Vol. 62, № 11. – P. 1458–1469.

REFERENCES

1. Boroznina N.P., Zaporotskova I.V., Boroznin S.V. Comparative Analysis of Sensor Activity of Carbon Nanotubes Modified with Functional Groups. *Journal of Nano- and Electronic Physics*, 2017, vol. 9, art. 03046.
2. Boroznina N.P., Zaporotskova I.V. Modeling the Sensing Activity of Carbon Nanotubes Functionalized with the Carboxyl, Amino, or Nitro Group Toward Alkali Metals. *Russian Microelectronics*, 2017, vol. 46, pp. 580–584.
3. Boroznina N.P., Zaporotskova I.V., Boroznin S.V. Sensitivity of Carboxyl-Modified Carbon Nanotubes to Alkaline Metals. *Nanosystems: physic, chemistry, mathematics*, 2018, vol. 9, pp. 79–84.
4. Abdelhalim A., Winkler M., Loghin F., Zeiser C., Lugli P., Abdellah A. Highly Sensitive and Selective Carbon Nanotube-Based Gas Sensor Arrays Functionalized with Different Metallic Nanoparticles. *Sens. Actuators B Chem.*, 2015, vol. 220, pp. 1288–1296.
5. Ding D., Chen Z., Rajaputra S., Singh V. Hydrogen Sensors Based on Aligned Carbon Nanotubes in an Anodic Aluminum Oxide Template with Palladium as a Top Electrode. *Sens. Actuators B Chem.*, 2007, vol. 124, pp. 12–17.
6. Penza M., Rossi R., Alvisi M., Serra E. Metal-Modified and Vertically Aligned Carbon Nanotube Sensors Array for Landfill Gas Monitoring Applications. *Nanotechnology*, 2010, vol. 21, art. 105501.
7. Leghrib R., Felten A., Demoisson F., Reniers F., Pireaux J.-J., Llobet E. Room-Temperature, Selective Detection of Benzene at Trace Levels Using Plasma-Treated Metal-Decorated Multiwalled Carbon Nanotubes. *Carbon*, 2010, vol. 48, pp. 3477–3484.
8. Boroznina N.P., Zaporotskova I.V., Boroznin S.V., Dryuchkov E.S. Sensors Based on Amino Group Surface-Modified CNTs. *Chemosensors*, 2019, vol. 7, pp. 1–7.
9. Huang C., Huang B., Jang Y., Tsai M., Yeh C. Three-Terminal CNTS Gas Sensor for N₂ Detection. *Diam. Relat. Mater.*, 2005, vol. 14, pp. 19–24.
10. Kauffman D.R., Sorescu D.C., Schofield D.P., Allen B.L., Jordan K.D., Star A. Understanding the Sensor Response of Metal-Decorated Carbon Nanotubes. *Nano Lett.*, 2010, vol. 10, pp. 958–963.
11. Zaporotskova I.V., Kozhitov L. V., Boroznina N.P. Sensor Activity with Respect to Alkali Metals of a Carbon Nanotube Edge-Modified with Amino Group. *Russ. J. Inorg. Chem.*, 2017, vol. 62, pp. 1458–1469.

INVESTIGATION OF THE INTERACTION OF CARBON DIOXIDE WITH MODIFIED FUNCTIONAL GROUPS OF NANOTUBES ¹

Lev V. Kozhitov

Doctor of Sciences (Engineering), Professor,
Department of Technology of Electronic Materials,
National Research Technological University “MISIS”
kozhitov@misis.ru
Prosp. Leninsky, 4, 119049 Moscow, Russian Federation

Irina V. Zaporotskova

Doctor of Sciences (Physics and Mathematics), Professor,
Director, Institute of Priority Technologies,
Volgograd State University
sefm@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Natalia P. Boroznina

Candidate of Sciences (Physics and Mathematics), Professor,
Department of Forensic Science and Physical Materials Science,
Volgograd State University
boroznina.natalya@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Sergey V. Boroznin

Candidate of Sciences (Physics and Mathematics), Associate Professor,
Department of Forensic Science and Physical Materials Science,
Volgograd State University
boroznin@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vladimir V. Akatiev

Senior Lecturer, Associate Professor,
Department of Forensic Science and Physical Materials Science,
Volgograd State University
sefm@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article presents a theoretical study of the possibility of interaction of one of the most common substances in nature – carbon dioxide – with modified functional carboxyl and amine groups of carbon nanotubes and borocarbon nanotubes of the BC5 type. The article analyzes the results of the interaction and provides a comparative analysis of the efficiency of the sorption interaction of a nanosystem with a carbon dioxide molecule. The performed studies prove the implementation of a weak physical sorption interaction between a nanosystem consisting of a carbon nanotube, a boundary-modified amine group, and a carbon dioxide molecule. This allows us talking about a possible sensory interaction that will allow

using such a complex to detect a micro amount of a substance-carbon dioxide. Based on this, it can be concluded that modified carbon nanotubes can be elements of sensors for determining the quality of indoor air, act as probes for cantilevers of atomic force microscopes and other devices. Recommendations are given for further use of the results as a basis for creating a highly sensitive new-generation sensor device for detecting micro-quantities of substances.

Key words: nanotubes, sensor devices, carbon dioxide molecule, sorption interaction, modification.



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2020.4.6>

УДК 544.723

ББК 24.5

ВЫЯВЛЕНИЕ ПРИМЕСЕЙ В ВОДЕ С ПОМОЩЬЮ НАНОСТРУКТУР

Олеся Александровна Какорина

Кандидат физико-математических наук,
доцент кафедры информационной безопасности,
Волгоградский государственный университет
sefm@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Игорь Александрович Какорин

Студент кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
sefm@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Александра Николаевна Панченко

Студент кафедры судебной экспертизы и физического материаловедения,
Волгоградский государственный университет
sefm@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе показана возможность адсорбции молекулы селитры на поверхности углеродных нанотрубок. Полученные результаты и применяемые методики могут быть использованы при проведении комплексных высокоэффективных экспертиз воды.

Ключевые слова: нанотрубки, адсорбция, молекула селитры, экспертиза воды, квантово-химические расчеты.

В жизни человека, растительного мира, животного и природы в целом вода играет чрезвычайно важную роль. Две трети поверхности планеты занимают моря и океаны. В природе вода пребывает в постоянном круговороте, на качество воды огромное влияние оказывает сельское хозяйство и промышленность. Не для кого не секрет, что для получения богатого урожая используют удобрения, основным компонентом которого является селитра. Вслед-

ствие этого в подземных водах и водоемах расположенных в непосредственной близости с полями обнаруживается селитра.

Селитра негативно влияет на организм человека, она способствует образованию опасного вещества в крови – метгемоглобина, который приводит к кислородному голоданию. Увеличение метгемоглобина до 60 % приводит к летальному исходу. Так же превышение селитры в воде становится причи-

ной отравления, нарушения в работе ЖКТ, выделительной и эндокринной системы, разрушение зубной эмали и появления кариеса. Определить селитру в воде можно путем химического анализа жидкости, а так же с помощью наноматериалов.

К наноматериалам относят структуры протяженностью менее 100 нм (нанометр, 10^{-9} м) в одном из измерений. На этом уровне материалы обладают уникальными, обусловленными размерами, свойствами (химическими, адсорбционными, каталитическими, магнитными, механическими, оптическими), определяющими высокую эффективность их использования в различных областях человеческой деятельности. В настоящее время более используемыми наноматериалами являются углеродные нанотрубки.

Углеродные нанотрубки (УНТ), открытые в 1991 г. [1] – это цилиндрические макромолекулы, представляющие собой гексагональную решетку атомов углерода, закрытые с торцов половиной молекулы фуллерена.

Данные структуры обладают достаточно высоко развитой адсорбционной поверхностью, это свойство и поможет выявить присутствие селитры в воде, одновременно и провести ее очистку.

Целью работы является изучение процесса адсорбции селитры на поверхности углеродного тубулена с помощью квантово-химических расчетов с применением полуэмпирической схемы MNDO.

Задачи:

1. Определить адсорбционный центр в калиевой и натриевой селитры.
2. Установить возможность с помощью УНТ определять примесь селитры в воде.

Объект исследования: вода содержащая примесь калиевой и натриевой селитр, углеродные нанотрубки.

Предмет: использование углеродных нанотрубок для выявления селитры в водопроводной воде.

Построение и расчет молекул калиевой и натриевой селитр

Для проведения теоретических расчетов взаимодействия углеродных нанотрубок с водой, содержащей примесь в виде селитры [4]. Необходимо было построить и выбрать оптимальную модель данной примеси. В работе рассматривалась калиевая селитра KNO_3 и натриевая селитра $NaNO_3$. Для определения оптимальной структуры были выполнены расчеты геометрии системы с использованием полуэмпирического метода MNDO в программном пакете Gamess. Расстояние между атомами N-O составляло $1,4 \text{ \AA}$, а между O-Me выбиралось равным $1,8 \text{ \AA}$. Структурные формулы калиевой и натриевой селитр представлены на рисунке 1. В результате расчетов были определены геометрические особенности данной структурной единицы (см. рис. 2). Так, установлено, что оптимальные расстояния между атомами N-O равно $1,22 \text{ \AA}$, атомами O-Na $1,9 \text{ \AA}$, а между O-K $2,2 \text{ \AA}$.

Исследование процесса адсорбции селитры на внешней поверхности УНТ

В качестве объекта исследования выбрана углеродная нанотрубка (6,6), которая моделировалась молекулярным кластером, расширенная элементарная ячейка (РЭЯ) которого содержала 216 атомов углерода. Расстояние между атомами углерода трубки составляет $1,4 \text{ \AA}$. Оборванные связи на границе кластера замыкались псевдоатомами водорода. Рассмотрены два положения молекулы селитры относительно

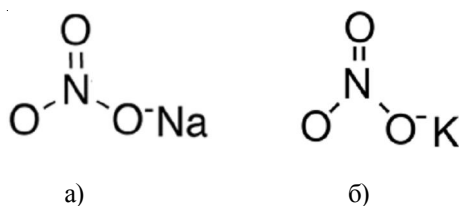


Рис. 1. Структурные формулы селитры:
а) натриевая селитра; б) калиевая селитра

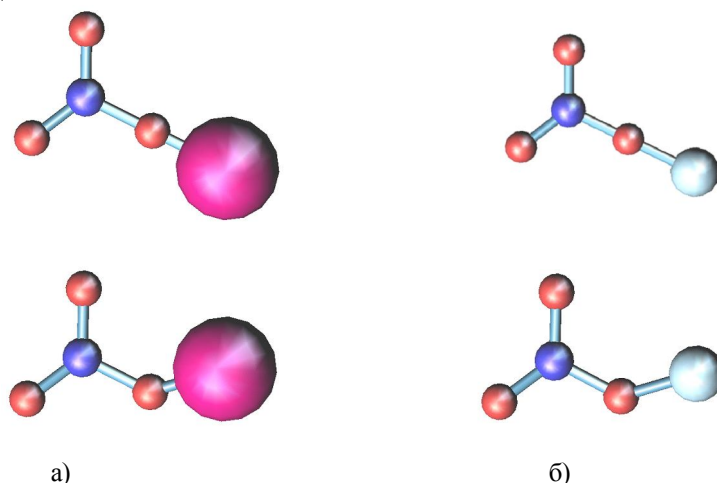


Рис. 2. Структурная формула селитры:

а) без оптимизации параметров; б) с оптимизацией параметров

но поверхности УНТ: 1) селитра ориентирована к трубке атомом металла; 2) селитра ориентирована к трубке атомами кислорода (рис. 3). Были рассмотрены два варианта ориентации молекулы: 1) над атомом углерода, 2) над центром углеродного гексагона.

Исследование процесса адсорбции молекулы селитры на внешней поверхности нанотрубки (6, 6) с использованием активного центра – атома металла

Рассмотрим процесс присоединения структурной единицы селитры к поверхности УНТ, используя активный центр – атом натрия или калия.

В первом варианте ориентации – над атомом углерода нанотрубки – молекула присоединялась к поверхностному атому углерода,

находящемуся примерно в середине кластера трубки, что позволило исключить влияние краевых эффектов. Процесс адсорбции моделировался пошаговым приближением молекулы селитры с шагом $0,1 \text{ \AA}$ к атому углерода поверхности вдоль перпендикуляра, проведенного через выбранный атом С. Геометрия системы оптимизировалась на каждом шаге. Выполненные расчеты позволили построить профили потенциальной энергии процессов адсорбции для калиевой и натриевой селитр. Анализ энергетической кривой установил, что селитра адсорбируются на поверхности трубки, что подтверждается наличием минимума на энергетических кривых, иллюстрирующего факт образования химической связи между атомом структурной единицы и атомом трубки. Реализуется так называемая химическая адсорбция, расстояния адсорбции составило для калиевой селитры $1,8 \text{ \AA}$, а для натриевой $1,6 \text{ \AA}$.



Рис. 3. Ориентация молекулы селитры относительно УНТ:

а) селитра ориентирована к трубке атомом металла; б) селитра ориентирована к трубке атомами кислорода

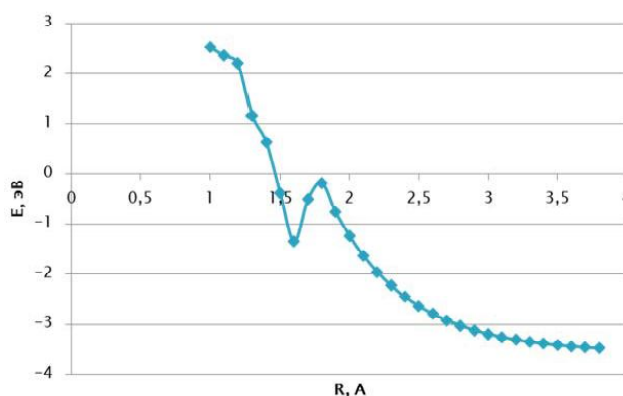
Выполненные расчеты при расположении молекулы селитры над центром углеродного гексагона позволили построить профиль энергии потенциальной энергии, как видно из графиков адсорбции селитры в этом случае не наблюдается, так как отсутствует энергетический минимум на кривой. Анализ геометрии показал, что происходит разрушение молекулы селитры, при этом атом металла попадает внутрь трубки и занимает устойчивое состояние на ее оси, при этом группа NO₃ адсорбиру-

ется на поверхности трубки. Следует заметить, что для калиевой селитры наблюдается химическая адсорбция, а для натриевой физическая адсорбция. Основные характеристики процессов адсорбции молекулы селитры на внешней поверхности нанотрубки (6, 6) с использованием активного центра – атома металла представлены в таблице 1.

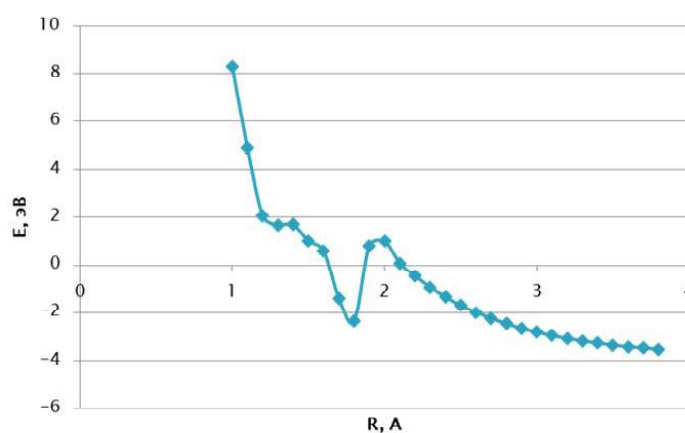
Анализ электронно-энергетического строения позволил построить одноэлектронные спектры комплекса «Селитра + УНТ» (рис. 4, 5).

Таблица 1

Вид селитры	Расположение адсорбционного центра-атома металла					
	Над атомом С			Над серединой гексагона		
	E_{ab} , эВ	$E_{ад}$, эВ	$R_{ад}$, Å	E_{ab} , эВ	$E_{ад}$, эВ	$R_{ад}$, Å
Натриевая	3,4	-1,34	1,6	–	–	–
Калиевая	4,7	-2,1	1,8	–	–	–



а)



б)

Рис. 4. Профиль поверхности потенциальной энергии взаимодействия селитры с углеродной нанотрубкой (6,6) для варианта 1 взаимодействия – адсорбционный центр-атом металла – расположен над атомом углерода:
а) натриевая селитра; б) калиевая селитра

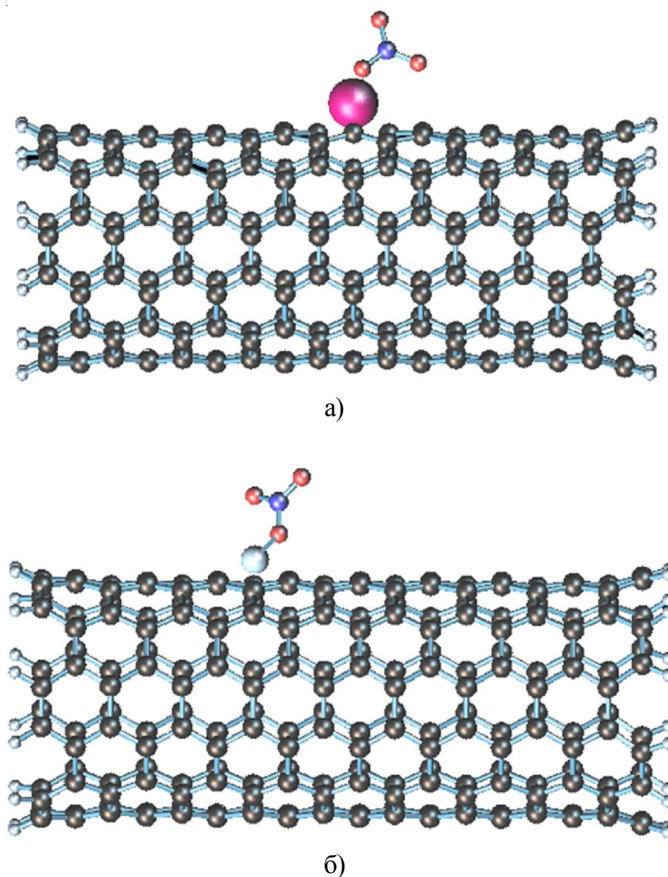


Рис. 5. Образование адсорбционного комплекса «Молекула селитры +УНТ»:

а) натриевая селитра; б) калиевая селитра

Была определена ширина запрещенной щели ΔE_g полученных структур как разность между энергиями верхней занятой и нижней вакантной орбиталей. Оказалось, что молекула селитры при адсорбции на поверхности углеродного тубулена приводит к уменьшению запрещенной зоны по сравнению с чистой УНТ.

Исследование процесса адсорбции селитры на внешней поверхности нанотрубки (6, б) с использованием активного центра – атомы кислорода

Далее был рассмотрен процесс присоединения селитры к поверхности УНТ, используя активный центр – атомы кислорода. Пошаговое приближение молекулы к трубке позволило построить профиль поверхности потенциальной энергии (см. рис. 6). Установлено, что молекула селитры в этом случае не адсорбируется на поверхности УНТ (см. рис. 7).

Атомно-эмиссионный анализ (АЭА) воды. Подготовка образцов для АЭА

Для проведения атомно-эмиссионного анализа было отобрано 5 образцов.

1 образец – 100 мл водопроводной воды

2 образец – 10 мл проточной воды с растворенной в ней 0,2 г калиевой селитры.

3 образец – 10 мл проточной воды с растворенной в ней 0,2 г натриевой селитры.

4 образец – 10 мл проточной воды с растворенной в ней 0,2 г калиевой селитры, пропущенной через фильтр с углеродными нанотрубками.

5 образец – 10 мл проточной воды с растворенной в ней 0,2 г натриевой селитры, пропущенной через фильтр с углеродными нанотрубками.

Все образцы готовились при помощи выпаривания. Выпаривание пробы воды производилось при температуре не более 90–95 °С на специальной установке, состоящей из элект-

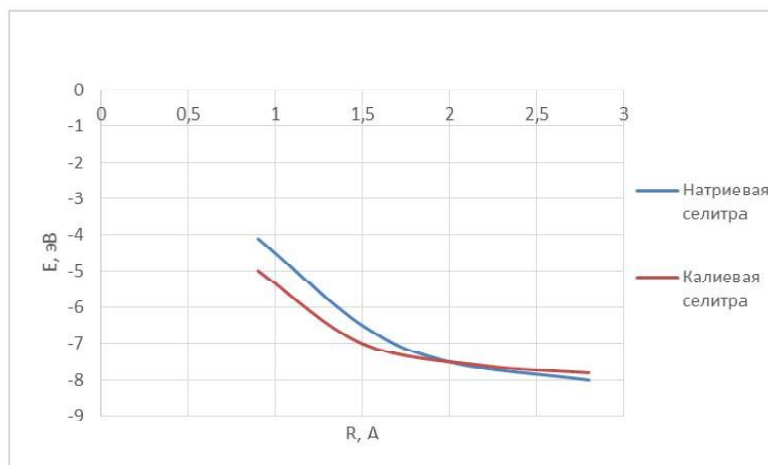


Рис. 6. Профиль поверхности потенциальной энергии взаимодействия селитры с углеродной нанотрубкой (6,6) для взаимодействия – адсорбционный центр-атомы кислорода

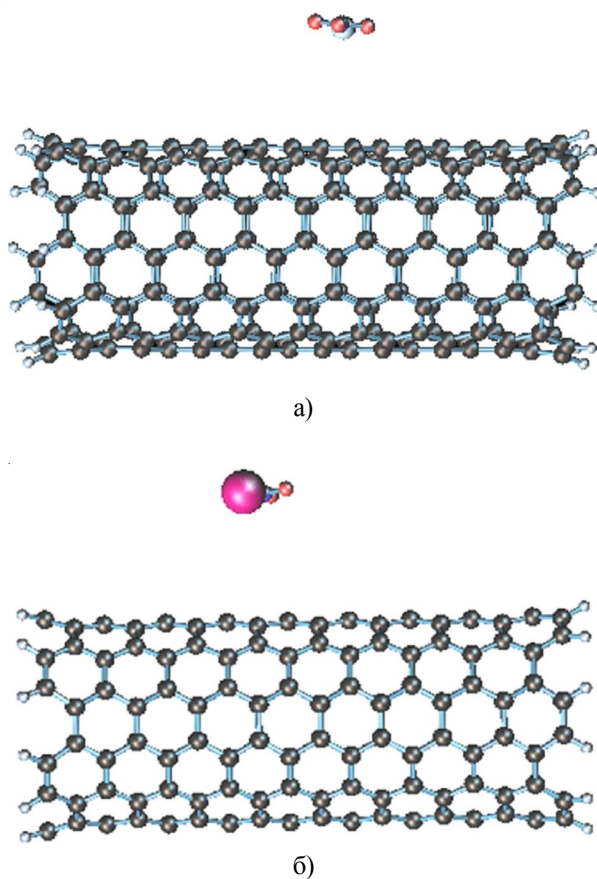


Рис. 7. Взаимодействие селитры с УНТ атомами кислорода:
а) калиевая селитра; б) натриевая селитра

троплитки, на которую устанавливается фарфоровая чашка, в которую наливается вода [2]. После выпаривания воды в чашке остается осадок, который используется в качестве образцов для АЭА.

Исследование воды методом атомно-эмиссионного анализ (АЭА)

Перед фокусировкой спектрографа необходимо произвести подготовку электродов

к работе. Концы железных (алюминиевых, медных, латунных) электродов заточите на конус с помощью напильника, выделенного для этих целей. Необходимо следить, чтобы поверхность пробы не оказалась загрязненной металлом, оставленным на инструменте предыдущей пробой. При заточке образцов напильниками для каждого вида продукции должен быть отдельный напильник. На заточенной поверхности не должно быть трещин и посторонних включений, так как они могут попасть в поле действия разряда и сильно исказить результаты анализа. Следят также за качеством заточки: зеркальная заточка позволяет заметно повысить воспроизводимость анализа.

Фокусировка спектрографа

Для правильного освещения спектрографа источник света должен быть установлен строго на оптической оси коллиматора, а оптическая ось конденсорной линзы должна совпадать с его осью. Установка дуги и конденсорной линзы выполняется следующим образом [2]:

1. Установка аналитического промежутка.

Для установки необходимого аналитического промежутка (до 3 мм) в камере разряда имеется специальная оптическая система, проектирующая на экран увеличенное в 3,5 раза теневое изображение рабочих концов электродов. По изображению контролируется правильность установки противоэлектрода или степень обгорания электродов. Эта

система позволяет совместить изображение середины аналитического промежутка (оптическую ось) с перекрестием сетки экрана, расположенного на передней панели камеры разряда.

Верхний электрод устанавливается с помощью держателя верхнего электрода (рис. 8), на котором закреплены неподвижная губка 1, подвижная губка 2, быстродействующий зажим 3. Для точного вывода оси противоэлектрода на оптическую ось спектрального аппарата при использовании различных противоэлектродов 4 предусмотрен поворот колодки 5 вокруг оси рукояткой эксцентрика 6. Требуемое положение противоэлектрода фиксируется гайкой 7. Откидной упор 9 поворачивается вокруг оси 8 и может занимать два положения: рабочее, при котором площадка 13 находится на оптической оси; и нерабочее, при котором площадка отведена на 90°. Правильность рабочего положения откидного упора регулируется винтом 10. Откидной упор позволяет осуществлять быструю и точную установку рабочего конца электрода 4 от оптической оси спектрального аппарата на расстояние половины аналитического промежутка, чтобы середина промежутка находилась на оптической оси. При вращении гайки 11 с кольцом 12 ось 8 вместе с откидным упором 9 и площадкой 13 под действием пружины 14 перемещается относительно оптической оси спектрального аппарата. Отсчет производится по шкале кольца и индексу-риске на наконечнике 15.

Цена деления шкалы кольца 12 равна 0,1 мм, один оборот кольца равен 1 мм. Коль-

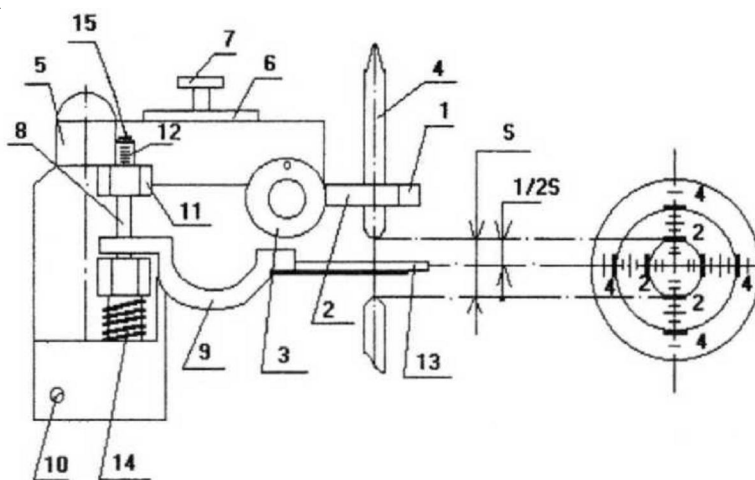


Рис. 8. Держатель верхнего электрода

цо 12 закрепляется к гайке 11 двумя винтами при нулевом положении шкалы (рабочая поверхность площадки 13 находится на оптической оси) [3]:

а) Установить верхний электрод на расстоянии 0,5S (S = 2 мм) (в качестве электродов используются железные стержни);

б) Установить нижний электрод, в котором находится исследуемый образец.

Методом ЭСА были исследованы все образцы воды и установлен элементный состав всех образцов. Основные химические элементы представлены в таблице 2.

Результаты выполненных исследований позволили установить, что после пропускания воды с примесью селитры, концентрация последней уменьшалась. Таким образом были подтверждены теоретические расчеты, показывающие возможность адсорбции селитры углеродными нанотрубками.

Основные результаты и выводы

1. Квантово-химические расчеты установили возможность адсорбции молекулы селитры на поверхности УНТ.

2. Атомно-эмиссионный анализ позволил установить, что при взаимодействии воды, содержащей примесь селитры с углеродными наноструктурами, количество данного вещества уменьшается.

3. Выполненные расчеты установили, что образовавшиеся адсорбционные комплексы «УНТ + селитра» обладают различными электронно-энергетическими характеристиками по сравнению с чистыми тубуленами. Это проявляется в изменении ширины запрещен-

ной зоны, что как раз и позволяет выявить данную примесь в воде.

4. Полученные результаты и применяемые методики могут быть использованы при проведении комплексных высокоэффективных экспертиз воды.

СПИСОК ЛИТЕРАТУРЫ

1. Дьячков, П. Н. Углеродные нанотрубки: строение, свойства, применения / П. Н. Дьячков. – М. : Бинум, 2006. – 293 с.
2. Запороцкова, И. В. Углеродные и неуглеродные наноматериалы и композитные структуры на их основе: Структура и электронные свойства : монография / И. В. Запороцкова. – Волгоград : Изд-во ВолГУ, 2009. – 490 с.
3. Эварестов, Р. А. Квантово-химические методы в теории твердого тела / Р. А. Эварестов. – Ленинград : ЛГУ, 1982. – 280 с.
4. Li., Quan-long. Исследование очищенных многостеночных углеродных нанотрубок в качестве сорбента твердофазной экстракции для предконцентрирования органофосфорных пестицидов из водных образцов / Quan-long Li , Dong-xing Yuan // Xiamen daxue xuebao. Ziran kexue ban = J. Xiamen Univ. Natur. Sci. – 2004. – Vol. 43, № 4. – С. 531–536.

REFERENCES

1. D'yachkov P.N. *Uglerodnye nanotrubki: stroenie, svojstva, primeneniya* [Carbon Nanotubes: Structure, Properties, applications]. Moscow, Binom Publ., 2006. 293 p.
2. Zaporockova, I.V. *Uglerodnye i neuglerodnye nanomaterialy i kompozitnye struktury na ih osnove: Struktura i elektronnye svojstva* [Carbon and Non-Carbon Nanomaterials and Composite Structures

Таблица 2

Элементный состав образцов

№	Образец	Элементный состав
1	Водопроводная вода	Ti, Ni, Zr, Co, Re, Sc, Ge
2	Раствор KNO ₃ + H ₂ O	K, Ge, Ca, Co, Si, Mg, Mn, Cu, Mo, Nb, As, Hf, Sn, Pr, Pt, Pb, Sc, Sb, Ta, Tb, Hg, Hf, Tl, Ti, P, Zr, Zn
3	Раствор NaNO ₃ + H ₂ O	Be, V, Bi, W, Gd, Ge, Au, Cd, Ca, Co, Re, Rh, U, Si, Mg, Mn, Cu, Mo, Na, Nb, Ni, Sn, Pr, Pt, Pb, Sc, Sr, Sb, Te, Ta, Th, Hg, Hf, Tl, Ti, P, Cr, Zn
4	Раствор KNO ₃ + H ₂ O после УНТ	Ge, Ca, Co, Si, Mg, Mn, Cu, Mo, Nb, As, Hf, Sn, Pr, Pt, Pb, Sc, Sb, Ta, Th, Hg, Hf, Tl, Ti, P, Zr, Zn
5	Раствор NaNO ₃ + H ₂ O после УНТ	Be, V, Bi, W, Gd, Ge, Au, Cd, Ca, Co, Re, Rh, U, Si, Mg, Mn, Cu, Mo, Nb, Ni, Sn, Pr, Pt, Pb, Sc, Sr, Sb, Te, Ta, Th, Hg, Hf, Tl, Ti, P, Cr, Zn

Based on Them: Structure and Electronic Properties]. Volgograd, Izd-vo VolGU, 2009. 490 p.

3. Evarestov R.A. *Kvantovo-himicheskie metody v teorii tverdogo tela* [Quantum Chemical Methods in Solid State Theory]. Leningrad, LGU, 1982. 280 p.

4. Li Quan-long, Yuan Dong-xing. Issledovanie ochishchennyh mnogostenochnyh uglerodnyh

nanotrubok v kachestve sorbenta tverdogaznoj ekstrakcii dlya predkonzentrirovaniya organofosfornyh pesticidov iz vodnyh obrazcov [Study of Purified Multi-Wall Carbon Nanotubes as a Solid-Phase Extraction Sorbent for the Preconcentration of Organophosphoric Pesticides from Water Samples]. *Xiamen daxue xuebao. Ziran kexue ban = J. Xiamen Univ. Natur. Sci.*, 2004, vol. 43, no. 4, pp. 531-536.

DETECTION OF IMPURITIES IN WATER USING NANOSTRUCTURES

Olesia A. Kakorina

Candidate of Sciences (Physics and Mathematics), Associate Professor,
Department of Information Security,
Volgograd State University
sefm@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Igor A. Kakorin

Student, Department of Forensic Science and Physical Materials Science,
Volgograd State University
sefm@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Alexandra N. Panchenko

Student, Department of Forensic Science and Physical Materials Science,
Volgograd State University
sefm@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Saltpeter negatively affects the human body, it contributes to the formation of a dangerous substance in the blood – methemoglobin, which leads to oxygen starvation. An increase in methemoglobin up to 60% leads to a fatal outcome. Also, the excess of saltpeter in water causes poisoning, disorders of the gastrointestinal tract, excretory and endocrine systems, the destruction of tooth enamel and the appearance of caries. Saltpeter can be determined in water by chemical analysis of the liquid, as well as using nanomaterials. These structures have a sufficiently highly developed adsorption surface, this property helps to detect the presence of saltpeter in water, and at the same time to clean it. The results of the studies made it possible to establish that after passing water with an admixture of saltpeter, the concentration of the latter decreased. Thus, the theoretical calculations showing the possibility of saltpeter adsorption by carbon nanotubes were confirmed. The obtained results and the applied methods can be used in conducting complex high-performance water examinations.

Key words: nanotubes, adsorption, saltpeter molecule, water analysis, quantum chemical calculations.

Журнал «НБИ технологии» издается для широкого ознакомления научной общественности с результатами современных исследований, посвященных вопросам развития инновационной деятельности, защиты объектов интеллектуальной собственности и ее коммерциализации, государственной политики в сфере управления инновациями, а также реализации инновационных технологий обучения.



Авторами «НБИ технологии» могут быть преподаватели, научные сотрудники и аспиранты высших учебных заведений и научно-исследовательских учреждений России, а также другие отечественные и зарубежные исследователи.

Уважаемые читатели!

Подписка на I полугодие 2021 года осуществляется по «Объединенному каталогу. Пресса России. Газеты и журналы». Т. 1. Подписной индекс 10384.

Стоимость подписки на I полугодие 2021 года 1 024 руб. 42 коп.
Распространение журнала осуществляется по адресной системе.

ТРЕБОВАНИЯ К СТАТЬЯМ, ПРЕДСТАВЛЯЕМЫМ В РЕДКОЛЛЕГИЮ ЖУРНАЛА «НБИ ТЕХНОЛОГИИ»

1. Материалы представляются на бумажном и электронном носителях по адресу: 400062, г. Волгоград, просп. Университетский, 100, Волгоградский государственный университет – главному редактору Запороцкой Ирине Владимировне или высылаются по электронной почте на адреса: vestnik10@volsu.ru.

Обязательно наличие сопроводительного письма, в котором должны содержаться следующие пункты: гарантия оригинальности статьи, отсутствия в ней недостоверных данных и плагиата; обязательство не подавать данный материал в другой журнал; информация о наличии/отсутствии потенциального конфликта интересов с членами редколлегии; данные о финансировании исследования (с пометкой об их конфиденциальности или необходимости опубликования); согласие с принципами, изложенными в разделе «Издательская этика» журнала (<https://ti.jvolsu.com/index.php/publishing-ethics-ru>).

Для российских авторов (аспирантов и соискателей ученой степени кандидата наук) необходимо дополнительно представить рекомендацию, подписанную научным руководителем и заверенную печатью учреждения.

2. Правила оформления статей.

Объем статьи не должен превышать 1 п. л.

Каждая статья должна включать следующие элементы издательского оформления:

- 1) Индексы УДК и ББК.
- 2) Заглавие. Подзаголовочные данные (на русском и английском языках).
- 3) Имя, отчество, фамилия автора; ученое звание, ученая степень; контактная информация (место работы/учебы и должность автора, полный почтовый адрес организации, телефон, e-mail) на русском и английском языках.
- 4) Аннотация на русском языке и авторское резюме (Abstract) на английском языке.
- 5) 5–8 ключевых слов или словосочетаний (на русском и английском языках).
- 6) Текст статьи.
- 7) Список литературы на русском языке, оформленный в соответствии с ГОСТ Р 7.1-2003, и References – список литературы на английском языке (латинским шрифтом), оформленный в соответствии с требованиями редакции. При необходимости – примечания, приложения.

2.1. Требования к авторским оригиналам на бумажном и электронном носителях:

- 1) Поля по 2 см с каждой стороны.
- 2) Нумерация страницы по центру внизу.
- 3) Шрифт Times New Roman, кегль 14, междустрочный интервал 1,5.
- 4) Файл должен быть создан в программе «Microsoft Word» и сохранен с расширением *.rtf; имя файла должно быть набрано латиницей и отражать фамилию автора.

2.2. Оформление библиографических ссылок и примечаний:

- 1) Библиографические ссылки на пристатейный список литературы должны быть оформлены с указанием в строке текста в квадратных скобках цифрового порядкового номера источника и через запятую номеров соответствующих страниц.
- 2) Пристатейный список литературы, озаглавленный как «Список литературы», составляется в алфавитном пронумерованном порядке. Он должен быть оформлен согласно ГОСТ 7.1–2003 с указанием обязательных сведений библиографического описания.

3. После получения материалов рукопись направляется на рецензирование. Решение о публикации статей принимается редакционной коллегией после рецензирования. Редакция оставляет за собой право отклонить или отправить представленные статьи на доработку на основании соответствующих заключений рецензентов. После получения положительной рецензии редакция уведомляет авторов о том, что статья принята к опубликованию, а также направляет замечания рецензентов и редакторов, в соответствии с которыми необходимо исправить или дополнить статью. В случае отказа в публикации статьи редакция представляет автору мотивированный отказ.

Полнотекстовые версии опубликованных статей и их метаданные (аннотации, ключевые слова, информация об авторах на русском и английском языках, список литературы) будут размещены в свободном доступе в Интернете на официальном сайте издания, на платформе Научной электронной библиотеки eLIBRARY.RU и других реферативных баз данных.

4. Более подробно с требованиями к статьям можно ознакомиться на страничке Издательства на сайте Волгоградского государственного университета: <https://www.volsu.ru> – и сайте журнала: <https://ti.jvolsu.com>.

ISSN 2658-3593



39 >

9 772658 359007