

2017
DECEMBER
№10 (32)

ISSN 2410-2865

EUROPEAN SCIENCE

[HTTP://SCIENTIFIC-PUBLICATION.COM](http://scientific-publication.com)

UNIVERSIDADE DE COIMBRA

**INSE PHOTOCONDUCTIVITY
BEYOND FUNDAMENTAL
ABSORPTION EDGE**
(Aliyeva A.M.) p.5

**STUDY OF BIOHUMUS
HUMIC ACIDS EXTRACTED
FROM BOTTOM SEDIMENTS**
(Yesenbayeva Zh.Zh.
Baihamurova M.O.) p.10

**THE IMMUNE STATUS IN
PATIENTS OF DUODENAL
ULCER DISEASES AND
THE INFLUENCE ON ITS
ERADICATIONAL AND
IMMUNOMODULATORY
THERAPY**
(Suleymanov S.F.) p.53



9 772410 286008

SCIENTIFIC PUBLISHING «PROBLEMS OF SCIENCE»

EUROPEAN SCIENCE

2017. № 10 (32)

EDITOR IN CHIEF
Valtsev S.

EDITORIAL BOARD

Abdullaev K. (PhD in Economics, Azerbaijan), *Alieva V.* (PhD in Philosophy, Republic of Uzbekistan), *Akbulayev N.* (D.Sc. in Economics, Azerbaijan), *Alikulov S.* (D.Sc. in Engineering, Republic of Uzbekistan), *Anan'eva E.* (D.Sc. in Philosophy, Ukraine), *Asaturova A.* (PhD in Medicine, Russian Federation), *Askarhodzhaev N.* (PhD in Biological Sc., Republic of Uzbekistan), *Bajtasov R.* (PhD in Agricultural Sc., Belarus), *Bakiko I.* (PhD in Physical Education and Sport, Ukraine), *Bahor T.* (PhD in Philology, Russian Federation), *Baulina M.* (PhD in Pedagogic Sc., Russian Federation), *Blejh N.* (D.Sc. in Historical Sc., PhD in Pedagogic Sc., Russian Federation), *Bogomolov A.* (PhD in Engineering, Russian Federation), *Borodaj V.* (Doctor of Social Sciences, Russian Federation), *Volkov A.* (D.Sc. in Economics, Russian Federation), *Gavrilenkova I.* (PhD in Pedagogic Sc., Russian Federation), *Garagonich V.* (D.Sc. in Historical Sc., Ukraine), *Glushhenko A.* (D.Sc. in Physical and Mathematical Sciences, Russian Federation), *Grinchenko V.* (PhD in Engineering, Russian Federation), *Gubareva T.* (PhD Laws, Russian Federation), *Gutnikova A.* (PhD in Philology, Ukraine), *Datij A.* (Doctor of Medicine, Russian Federation), *Demchuk N.* (PhD in Economics, Ukraine), *Divnenko O.* (PhD in Pedagogic Sc., Russian Federation), *Dolenko G.* (D.Sc. in Chemistry, Russian Federation), *Esenova K.* (D.Sc. in Philology, Kazakhstan), *Zhamuldinov V.* (PhD Laws, Kazakhstan), *Zholdoshev S.* (Doctor of Medicine, Republic of Kyrgyzstan), *Ibadov R.* (D.Sc. in Physical and Mathematical Sciences, Republic of Uzbekistan), *Il'inskih N.* (D.Sc. Biological, Russian Federation), *Kajrakbaev A.* (PhD in Physical and Mathematical Sciences, Kazakhstan), *Kaftaeva M.* (D.Sc. in Engineering, Russian Federation), *Koblanov Zh.* (PhD in Philology, Kazakhstan), *Kovaljov M.* (PhD in Economics, Belarus), *Kravcova T.* (PhD in Psychology, Kazakhstan), *Kuz'min S.* (D.Sc. in Geography, Russian Federation), *Kulikova E.* (D.Sc. in Philology, Russian Federation), *Kurmanbaeva M.* (D.Sc. Biological, Kazakhstan), *Kurpajanidi K.* (PhD in Economics, Republic of Uzbekistan), *Linkova-Daniels N.* (PhD in Pedagogic Sc., Australia), *Lukienko L.* (D.Sc. in Engineering, Russian Federation), *Makarov A.* (D.Sc. in Philology, Russian Federation), *Macarenko T.* (PhD in Pedagogic Sc., Russian Federation), *Meimanov B.* (D.Sc. in Economics, Republic of Kyrgyzstan), *Muradov Sh.* (D.Sc. in Engineering, Republic of Uzbekistan), *Nabiev A.* (D.Sc. in Geoinformatics, Azerbaijan), *Nazarov R.* (PhD in Philosophy, Republic of Uzbekistan), *Naumov V.* (D.Sc. in Engineering, Russian Federation), *Ovchinnikov Ju.* (PhD in Engineering, Russian Federation), *Petrov V.* (D.Arts, Russian Federation), *Radkevich M.* (D.Sc. in Engineering, Republic of Uzbekistan), *Rakhimbekov S.* (D.Sc. in Engineering, Kazakhstan), *Rozyhodzhaeva G.* (Doctor of Medicine, Republic of Uzbekistan), *Romanenkova Yu.* (D.Arts, Ukraine), *Rubcova M.* (Doctor of Social Sciences, Russian Federation), *Rumyantsev D.* (D.Sc. in Biological Sc., Russian Federation), *Samkov A.* (D.Sc. in Engineering, Russian Federation), *San'kov P.* (PhD in Engineering, Ukraine), *Selitrenikova T.* (D.Sc. in Pedagogic Sc., Russian Federation), *Sibircev V.* (D.Sc. in Economics, Russian Federation), *Skripko T.* (D.Sc. in Economics, Ukraine), *Sopov A.* (D.Sc. in Historical Sc., Russian Federation), *Strekalov V.* (D.Sc. in Physical and Mathematical Sciences, Russian Federation), *Stukalenko N.M.* (D.Sc. in Pedagogic Sc., Kazakhstan), *Subachev Ju.* (PhD in Engineering, Russian Federation), *Sulejmanov S.* (PhD in Medicine, Republic of Uzbekistan), *Tregub I.* (D.Sc. in Economics, PhD in Engineering, Russian Federation), *Uporov I.* (PhD Laws, D.Sc. in Historical Sc., Russian Federation), *Fedos'kina L.* (PhD in Economics, Russian Federation), *Khiltukhina E.* (D.Sc. in Philosophy, Russian Federation), *Cuculjan S.* (PhD in Economics, Republic of Armenia), *Chiladze G.* (Doctor of Laws, Georgia), *Shamshina I.* (PhD in Pedagogic Sc., Russian Federation), *Sharipov M.* (PhD in Engineering, Republic of Uzbekistan), *Shevko D.* (PhD in Engineering, Russian Federation).

Publishing house «PROBLEMS OF SCIENCE»

Founded in 2009. Ten times a year

EDITORIAL OFFICE ADDRESS:

153008, Russian Federation, Ivanovo, Lezhnevskaya st., h.55, 4th floor

Phone: +7 (910) 690-15-09.

<http://scientific-publication.com> / e-mail: info@p8n.ru

Moscow

2017

EUROPEAN SCIENCE

2017. № 10 (32)

ГЛАВНЫЙ РЕДАКТОР: Вальцев С.В.

Заместитель главного редактора: Ефимова А.В.

РЕДАКЦИОННЫЙ СОВЕТ:

Выходит 10 раз в год

Подписано в печать:

11.12.2017

Дата выхода в свет:

13.12.2017

Формат 70x100/16.

Бумага офсетная.

Гарнитура «Таймс».

Печать офсетная.

Усл. печ. л. 4,87

Тираж 1 000 экз.

Заказ № 1472

ИЗДАТЕЛЬСТВО

«Проблемы науки»

Территория

распространения:

зарубежные страны,

Российская

Федерация

Журнал

зарегистрирован

Федеральной службой

по надзору в сфере

связи,

информационных

технологий и

массовых

коммуникаций

(Роскомнадзор)

Свидетельство

ПИ № ФС77 - 60218

Издаётся с 2014 года

Абдуллаев К.Н. (д-р филос. по экон., Азербайджанская Республика), *Алиева В.Р.* (канд. филос. наук, Узбекистан), *Акбулаев Н.Н.* (д-р экон. наук, Азербайджанская Республика), *Аликулов С.Р.* (д-р техн. наук, Узбекистан), *Ананьева Е.П.* (д-р филос. наук, Украина), *Асатурова А.В.* (канд. мед. наук, Россия), *Аскарходжаев Н.А.* (канд. биол. наук, Узбекистан), *Байтасов Р.Р.* (канд. с.-х. наук, Белоруссия), *Бакико И.В.* (канд. наук по физ. воспитанию и спорту, Украина), *Бахор Т.А.* (канд. филол. наук, Россия), *Баулина М.В.* (канд. пед. наук, Россия), *Блейх Н.О.* (д-р ист. наук, канд. пед. наук, Россия), *Богомолов А.В.* (канд. техн. наук, Россия), *Бородай В.А.* (д-р социол. наук, Россия), *Волков А.Ю.* (д-р экон. наук, Россия), *Гавриленкова И.В.* (канд. пед. наук, Россия), *Гарагонич В.В.* (д-р ист. наук, Украина), *Глуценко А.Г.* (д-р физ.-мат. наук, Россия), *Гринченко В.А.* (канд. техн. наук, Россия), *Губарева Т.И.* (канд. юрид. наук, Россия), *Гутникова А.В.* (канд. филол. наук, Украина), *Датий А.В.* (д-р мед. наук, Россия), *Демчук Н.И.* (канд. экон. наук, Украина), *Дивненко О.В.* (канд. пед. наук, Россия), *Доленко Г.Н.* (д-р хим. наук, Россия), *Есенова К.У.* (д-р филол. наук, Казахстан), *Жамулдинов В.Н.* (канд. юрид. наук, Казахстан), *Жолдошев С.Т.* (д-р мед. наук, Кыргызская Республика), *Ибадов Р.М.* (д-р физ.-мат. наук, Узбекистан), *Ильинских Н.Н.* (д-р биол. наук, Россия), *Кайракбаев А.К.* (канд. физ.-мат. наук, Казахстан), *Кафтаева М.В.* (д-р техн. наук, Россия), *Киквидзе И.Д.* (д-р филол. наук, Грузия), *Кобланов Ж.Т.* (канд. филол. наук, Казахстан), *Ковалёв М.Н.* (канд. экон. наук, Белоруссия), *Кравцова Т.М.* (канд. психол. наук, Казахстан), *Кузьмин С.Б.* (д-р геогр. наук, Россия), *Куликова Э.Г.* (д-р филол. наук, Россия), *Курманбаева М.С.* (д-р биол. наук, Казахстан), *Курпаяниди К.И.* (канд. экон. наук, Узбекистан), *Линькова-Даниельс Н.А.* (канд. пед. наук, Австралия), *Лукиенко Л.В.* (д-р техн. наук, Россия), *Макаров А. Н.* (д-р филол. наук, Россия), *Мацаренко Т.Н.* (канд. пед. наук, Россия), *Мейманов Б.К.* (д-р экон. наук, Кыргызская Республика), *Мурадов Ш.О.* (д-р техн. наук, Узбекистан), *Набиев А.А.* (д-р наук по геоинформ., Азербайджанская Республика), *Назаров Р.Р.* (канд. филос. наук, Узбекистан), *Наумов В. А.* (д-р техн. наук, Россия), *Овчинников Ю.Д.* (канд. техн. наук, Россия), *Петров В.О.* (д-р искусствоведения, Россия), *Радкевич М.В.* (д-р техн. наук, Узбекистан), *Рахимбеков С.М.* (д-р техн. наук, Казахстан), *Розыходжаева Г.А.* (д-р мед. наук, Узбекистан), *Романенкова Ю.В.* (д-р искусствоведения, Украина), *Рубцова М.В.* (д-р. социол. наук, Россия), *Румянцев Д.Е.* (д-р биол. наук, Россия), *Самков А. В.* (д-р техн. наук, Россия), *Саньков П.Н.* (канд. техн. наук, Украина), *Селитреникова Т.А.* (д-р пед. наук, Россия), *Сибирцев В.А.* (д-р экон. наук, Россия), *Скрипо Т.А.* (д-р экон. наук, Украина), *Сонов А.В.* (д-р ист. наук, Россия), *Стрекалов В.Н.* (д-р физ.-мат. наук, Россия), *Стукаленко Н.М.* (д-р пед. наук, Казахстан), *Субачев Ю.В.* (канд. техн. наук, Россия), *Сулейманов С.Ф.* (канд. мед. наук, Узбекистан), *Трезуб И.В.* (д-р экон. наук, канд. техн. наук, Россия), *Упоров И.В.* (канд. юрид. наук, д-р ист. наук, Россия), *Федоськина Л.А.* (канд. экон. наук, Россия), *Хилтухина Е.Г.* (д-р филос. наук, Россия), *Цицулян С.В.* (канд. экон. наук, Республика Армения), *Чиадзе Г.Б.* (д-р юрид. наук, Грузия), *Шамшина И.Г.* (канд. пед. наук, Россия), *Шарипов М.С.* (канд. техн. наук, Узбекистан), *Шевко Д.Г.* (канд. техн. наук, Россия).

Свободная цена

© ЖУРНАЛ «EUROPEAN SCIENCE»
© ИЗДАТЕЛЬСТВО «ПРОБЛЕМЫ НАУКИ»

Содержание

PHYSICO-MATHEMATICAL SCIENCES	5
<i>Aliyeva A.M. (Republic of Azerbaijan) INSE PHOTOCONDUCTIVITY BEYOND FUNDAMENTAL ABSORPTION EDGE / Алиева А.М. (Азербайджанская Республика) ФОТОПРОВОДИМОСТЬ INSE ЗА КРАЕМ ФУНДАМЕНТАЛЬНОГО ПОГЛОЩЕНИЯ.....</i>	5
TECHNICAL SCIENCES.....	10
<i>Yesenbayeva Zh.Zh., Baihamurova M.O. (Republic of Kazakhstan) STUDY OF BIONUMUS HUMIC ACIDS EXTRACTED FROM BOTTOM SEDIMENTS / Есенбаева Ж.Ж., Байхамурова М.О. (Республика Казахстан) ИЗУЧЕНИЕ ГУМИНОВЫХ КИСЛОТ БИОГУМУСОВ, ПОЛУЧЕННЫХ ИЗ ДОННЫХ ОСАДКОВ</i>	10
<i>Kulchitsky A.P., Shalimov A.S., Timoshenkov A.S. (Russian Federation) OPTOELECTRONIC SYSTEM FOR AUTOMATIC LANDING OF UNMANNED SMALL AIRCRAFTS / Кульчицкий А.П., Шалимов А.С., Тимошенко А.С. (Российская Федерация) ОПТИКО-ЭЛЕКТРОННАЯ СИСТЕМА АВТОМАТИЧЕСКОЙ ПОСАДКИ БЕСПИЛОТНЫХ МАЛЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ</i>	13
<i>Nazarenko Yu.L. (Russian Federation) USE OF NEUROETRES FOR SOLVING CYBER SECURITY ISSUES / Назаренко Ю.Л. (Российская Федерация) ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ В РАМКАХ РЕШЕНИЯ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ</i>	19
<i>Nazarenko Yu.L. (Russian Federation) CRYPTO STABILITY OF GENERATORS OF RANDOM NUMBERS. YARROW ALGORITHM / Назаренко Ю.Л. (Российская Федерация) КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ. АЛГОРИТМ ЯРРОУ</i>	24
<i>Sinochkin D.V. (Russian Federation) CRYPTOANALYSIS OF CIPHER OF SIMPLE REPLACEMENT / Синочкин Д.В. (Российская Федерация) КРИПТОАНАЛИЗ ШИФРА ПРОСТОЙ ЗАМЕНЫ</i>	30
<i>Sinochkin D.V. (Russian Federation) MODIFICATIONS AND COMBINATION OF CODES SET BY A SIMPLE FLOAT / Синочкин Д.В. (Российская Федерация) МОДИФИКАЦИИ И КОМБИНИРОВАНИЕ КОДОВ, ЗАДАННЫХ НАД ПРОСТЫМ ПОЛЕМ</i>	33
<i>Sinochkin D.V. (Russian Federation) RSA CRYPTANALYSIS / Синочкин Д.В. (Российская Федерация) КРИПТОАНАЛИЗ RSA</i>	37
ECONOMICS	41
<i>Tolmachev A.V., Elagina A.S., Byzova V.E. (Russian Federation) THE ROLE OF MARKETING COMMUNICATIONS IN THE COMPANY / Толмачев А.В., Елагина А.С., Бызова В.Е. (Российская Федерация) РОЛЬ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ В КОМПАНИИ</i>	41

<i>Guliev Sh.R.</i> (Russian Federation) ANALYSIS OF THE INDEX OF BUSINESS EXPECTATIONS OF ENTREPRENEURS FROM STATE SUPPORT MEASURES / <i>Гулиев Ш.Р.</i> (Российская Федерация) АНАЛИЗ ИНДЕКСА БИЗНЕС-ОЖИДАНИЙ ПРЕДПРИНИМАТЕЛЕЙ ОТ МЕР ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ.....	44
<i>Guliev Sh.R.</i> (Russian Federation) THE DEVELOPMENT INSTRUMENTS OF COMPANIES ENGAGED IN INNOVATION ACTIVITIES / <i>Гулиев Ш.Р.</i> (Российская Федерация) ИНСТРУМЕНТЫ РАЗВИТИЯ КОМПАНИЙ, ОСУЩЕСТВЛЯЮЩИХ ИННОВАЦИОННУЮ ДЕЯТЕЛЬНОСТЬ	46
LEGAL SCIENCES.....	48
<i>Zharova A.G.</i> (Russian Federation) THE CONCEPT AND CHARACTERISTICS OF SELF-REGULATION INSTITUTE IN RUSSIAN FEDERATION / <i>Жарова А.Г.</i> (Российская Федерация) ПОНЯТИЕ И ОСОБЕННОСТИ ИНСТИТУТА САМОРЕГУЛИРОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ	48
MEDICAL SCIENCES	53
<i>Suleymanov S.F.</i> (Republic of Uzbekistan) THE IMMUNE STATUS IN PATIENTS OF DUODENAL ULCER DISEASES AND THE INFLUENCE ON ITS ERADICATIONAL AND IMMUNOMODULATORY THERAPY / <i>Сулейманов С.Ф.</i> (Республика Узбекистан) ИММУННЫЙ СТАТУС У БОЛЬНЫХ ЯЗВЕННОЙ БОЛЕЗНЬЮ ДВЕНАДЦАТИПЕРСТНОЙ КИШКИ И ВЛИЯНИЕ НА НЕЁ ЭРАДИКАЦИОННОЙ И ИММУНОМОДУЛИРУЮЩЕЙ ТЕРАПИИ.....	53
PSYCHOLOGICAL SCIENCES	57
<i>Tabakova V.P., Kurdyuk T.A.</i> (Russian Federation) INTELLECT OR EMOTIONAL INTELLIGENCE: WHICH COEFFICIENT DETERMINES SUCCESS IN OUR LIFE? / <i>Табакова В.П., Курдюк Т.А.</i> (Российская Федерация) ЭМОЦИОНАЛЬНЫЙ И ИНТЕЛЛЕКТУАЛЬНЫЙ КОЭФФИЦИЕНТЫ: КАКОЙ КОЭФФИЦИЕНТ ОПРЕДЕЛЯЕТ УСПЕХ В НАШЕЙ ЖИЗНИ?	57

INSE PHOTOCONDUCTIVITY BEYOND FUNDAMENTAL ABSORPTION EDGE

Aliyeva A.M. (Republic of Azerbaijan)

Email: Aliyeva432@scientifictext.ru

*Aliyeva Aytan Movsum gizi – PhD in Physics, Senior Researcher,
LABORATORY FOR TRANSPORT PHENOMENA IN SEMICONDUCTORS
AND NANOSTRUCTURES,
INSTITUTE OF PHYSICS
NATIONAL ACADEMY OF SCIENCES OF AZERBAIJAN,
BAKU, REPUBLIC OF AZERBAIJAN*

Abstract: in InSe layered crystals, photoconductivity has been experimentally observed beyond fundamental absorption. Radiation intensity was changed with use of calibrated neutral filters. The output of fundamental absorption signals was fed into non-stationary digital system, which included a storage oscilloscope and computer system. The measurements were conducted in the temperature range of 300 to 90K. With increasing intensity of the laser radiation, the photoconductivity maximum was clearly manifested, but with a further increase in intensity, its decrease occurred. Photoconductivity features in the range of high energies are explained by influence of hyperbolic excitons generated by the laser light.

Keywords: photoconductivity, exciton, fundamental absorption, Bridgman method, Brillion zone.

ФОТОПРОВОДИМОСТЬ INSE ЗА КРАЕМ ФУНДАМЕНТАЛЬНОГО ПОГЛОЩЕНИЯ Алиева А.М. (Азербайджанская Республика)

*Алиева Айтан Мовсум гызы – доктор философии, старший научный сотрудник,
лаборатория явлений переноса в полупроводниках и наноструктурах,
Институт физики
Национальной академии наук Азербайджана,
г. Баку, Азербайджанская Республика*

Аннотация: экспериментально установлена фотопроводимость в слоистых кристаллах InSe за краем фундаментального поглощения. Интенсивность излучения изменяли при помощи калиброванных нейтральных фильтров. Выход сигналов фотопроводимости подавали в нестационарную цифровую систему, которая включала запоминающий осциллограф и компьютерную систему. Измерения проводили в интервале температур 300–90K. С увеличением интенсивности лазерного излучения максимум фотопроводимости отчетливо проявлялся, но при дальнейшем увеличении интенсивности происходило его уменьшение. Особенности фотопроводимости в области больших энергий объясняются влиянием гиперболических экситонов, генерированных лазерным светом.

Ключевые слова: фотопроводимость, экситон, фундаментальное поглощение, метод Бриджмена, зона Бриллюэна.

УДК 541.49:661.43:535.37

ВВЕДЕНИЕ

Ранее нами в слоистых кристаллах InSe экспериментально исследовалось нелинейное поглощение света и его временная эволюция в области экситонного

резонанса у края основной полосы поглощения при высоких уровнях возбуждения [1]. Было показано, что наблюдаемая временная зависимость коэффициента поглощения и его зависимость от интенсивности возбуждения определяется экситон-экситонным взаимодействием и экранированием экситонов плазмой неравновесных носителей, генерированных лазерным светом. Длина экранирования, определенная по формуле Дебай-Хюгеля, оказалась равной $\sim 10 \text{ \AA}$, что меньше радиуса экситона в InSe $\sim 37 \text{ \AA}$.

Особый интерес представляет обнаружение нелинейного поглощения в кристаллах InSe за краем фундаментального поглощения (КФП). При проведении таких исследований необходимы очень тонкие образцы (микронной толщины) с относительно малым значением коэффициента оптического поглощения за КФП, отсутствие поверхностных дефектов, а также мощных источников света. На наш взгляд, слоистые кристаллы InSe являются удобным объектом для проведения таких исследований. В этих кристаллах между слоями имеется слабая ван-дер-ваальсова связь, что позволяет осуществить скол вдоль плоскости спайности и получить образцы с толщинами вплоть до долей микрона. Отсутствие оборванных связей практически исключает возможности образования поверхностных уровней (концентрация поверхностных состояний на два порядка меньше, чем в обычных полупроводниках), и эти кристаллы обладают высококачественными естественными зеркальными поверхностями. Коэффициент поглощения около края мал ($\alpha \sim 10^3 \text{ см}^{-1}$) по сравнению с другими полупроводниками ($\alpha \sim 10^4\text{--}10^5 \text{ см}^{-1}$).

Благодаря этим свойствам, удалось исследовать спектры поглощения кристаллов InSe за КФП [2, 3]. Анализ приведенных в [2, 3] данных показывает, что в исследуемой области спектр поглощения кристаллов InSe имеет две особенности:

- высокоэнергетическую, связанную с между зонными переходами в седловой точке типа M_1 , которая располагается в центре боковой грани зоны Бриллюэна;
- низкоэнергетическую, обусловленную образованием экситонов седловой точки (гиперболические экситоны).

В [4] наблюдалось резонансное излучение в InSe, обусловленное переходами из состояний, находящихся в глубине зоны проводимости и валентной зоны и расположенных на расстояниях, соизмеримых с шириной запрещенной зоны. Следует отметить, что гиперболические экситоны наряду со слоистыми кристаллами в настоящее время интенсивно исследуются и в других полупроводниках [5–8].

Цель данной работы – исследование неравновесной фотопроводимости (ФП) в кристаллах InSe за КФП. Спектры ФП слоистых полупроводников $A^{III}B^{VI}$ в области энергий $h\nu > E_g$ исследованы в [9, 10]. Однако эти измерения были проведены обычными (не лазерными) источниками света и при низких интенсивностях возбуждения.

ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ

Были исследованы монокристаллы InSe, выращенные методом Бриджмена. Толщина образцов составляла 2–10 мкм. Подвижность и концентрация электронов, определенные из холловских измерений, составили $1.2 \times 10^3 \text{ см}^2/(\text{В с})$ и $7 \times 10^{14} \text{ см}^{-3}$ соответственно. Омические контакты наносили напылением индия на освещенной поверхности образцов (перпендикулярно оптической оси С). Кристаллы облучали импульсами жидкостного лазера (активная среда роданом 6G), накачку которого осуществляли азотным лазером. Область перестройки длины волны излучения 473–547 нм, ширина линии генерации во всем диапазоне $\sim 0.4 \text{ \AA}$. Мощность импульса составляла 120 кВт при длительности 3 нс, а частота повторения импульса равна 20 Гц. Интенсивность излучения изменяли при помощи калиброванных нейтральных фильтров. Выход сигналов ФП подавали в нестационарную цифровую систему, которая включала запоминающий осциллограф и компьютерную систему. Измерения проводили в интервале температур 300–90 К.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

На рис.1 представлены спектры ФП кристаллов InSe при различных интенсивностях возбуждения. Как видно, при низких интенсивностях возбуждения (кривая 1) в спектре наблюдается слабая полоса с максимумом при 508 нм. С увеличением интенсивности лазерного излучения максимум ФП отчетливо проявляется (кривые 2 и 3), но при дальнейшем увеличении интенсивности происходит его уменьшение (кривая 4).

На рис. 2 приведены спектры ФП InSe при 300 (кривая 1) и 90 К (кривая 2). Видно, что уменьшение температуры до 90 К приводит к увеличению ФП более чем в 10 раз. Проведенные исследования показали, что кристаллы InSe обладают значительной фоточувствительностью за краем основной полосы поглощения. Максимумы в спектрах ФП полностью коррелируют с максимумами спектров поглощения и фотолуминесценции InSe, обусловленными гиперболическими экситонами [3, 4]. Резонансный характер максимума ФП свидетельствует об его экситонной природе. Об этом также свидетельствуют значительная полуширина спектров ФП, их стабильность и асимметрия с более коротковолновым краем.

Значительное увеличение ФП с уменьшением температуры, по-видимому, обусловлено изменением времени релаксации носителей тока с температурой. Анализ кинетических уравнений ФП при высоких уровнях оптического возбуждения рассмотрен в [11].

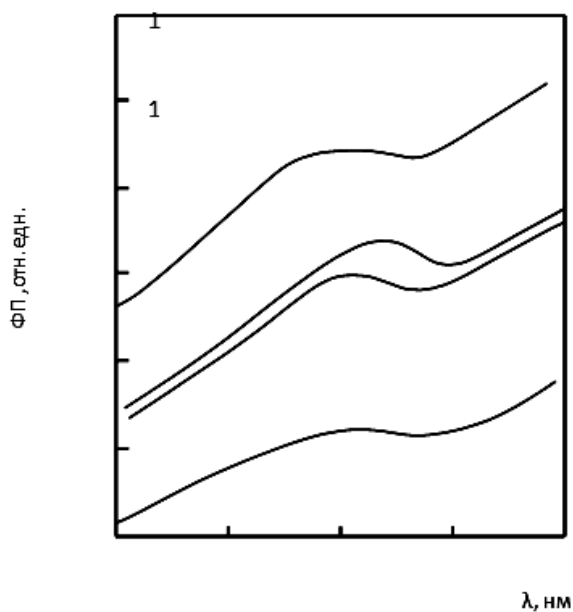


Рис. 1. Спектры ФП кристаллов InSe при интенсивностях возбуждения 1.34 (1), 3.74 (2), 6.4 (3), 12 МВт/см² (4)

Согласно [11], ФП, обусловленная экситонами, при низких уровнях возбуждения линейно изменяется с интенсивностью возбуждения, но при высоком уровне возбуждения, когда нелинейное поглощение становится доминирующим, ФП начинает снижаться. Наши экспериментальные данные, относящиеся к исследованию люкс-амперной характеристики ФП InSe, хорошо согласуются с результатами [11] до уровня возбуждения 6 МВт/см²; при более высоких уровнях возбуждения ФП начинает уменьшаться. Данное снижение ФП можно объяснить не только уменьшением экситонного поглощения, обусловленного процессом экранирования

экситонов свободными носителями, но и термическим гашением ФП и образованием поверхностных состояний при очень высоких уровнях оптического возбуждения.

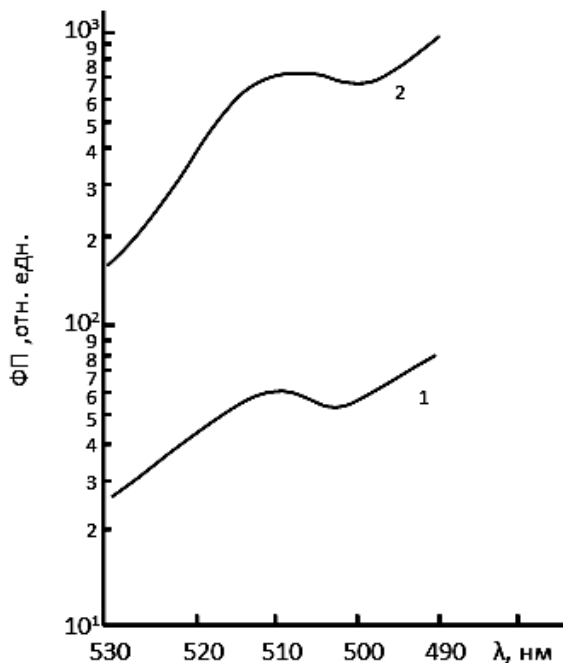


Рис. 2. Спектры ФП InSe при 300 (1) и 90 К (2) ($W = 12 \text{ МВм/см}^2$)

ЗАКЛЮЧЕНИЕ

Показано, что кристаллы InSe являются удобным объектом для исследования фотопроводимости за краем фундаментального поглощения при высоких уровнях возбуждения. Наличие значительной чувствительности в этой области свидетельствует о высоком качестве естественных поверхностных слоев и позволяет утверждать, что кристаллы InSe могут быть использованы в качестве фотоприемников не только в инфракрасной области спектра, а также в видимой области.

Список литературы / References

1. Кязым-заде А.Г., Агаева А.А., Салманов В.М., Мохтари А.Г. Неорганические материалы. 43, 2007. 1419.
2. Савчук А.И., Говалешко Н.Л., Далецкий Г.Д., Ковалюк З.Д. УФЖ. 17, 1972. 1548.
3. Абуталыбов Г.И., Белле М.Л., ФТП. 8, 1974. 2392.
4. Дворников Д.П., Салманов В.М., Ярошецкий И.Д. Письма в ЖЭТФ. 20, 1974. 17.
5. Вирко С.В., Лисица М.П., Моцный Ф.В. ФТТ. 42, 2000. 1579.
6. Белявский В.И., Кончаков Р.А. ФТТ. 43, 2001. 1558.
7. Крохмаль А.П. ФТП. 37, 2003. 257.
8. Канустянык В.Б., Пастернак Р.М., Калущ А.З., Панасюк М.Р., Цибульский В.С., Рудык В.П., Серкиз Р.Я. Журнал Прикладной Спектроскопии. 74, 2007. 252.
9. Segura A., Guesdon J.P., Besson J.M. J. Appl. Phys. 54, 1983. 876.
10. Alekperov O.Z., Godjaev M.O., Zarbaliev M.Z., Suleimanov R. Sol. Stat. Comm. 77, 1991. 65.
11. Egorov V.D., Müller G.O., Zimmermann R. Sol. Stat. Comm. 38, 1991. 271.

Список литературы на английском языке / References in English

1. *Kyazym-zade, A.G., Agaeva, A.A., Salmanov, V.M. et al.* Inorg Mater, 2007. 43:1275 .
2. *Savchuk A.I., Govareshko N.L., Dalevsky G.D., Kovaluk Z.D.* Ukrainian Physics Journal. 17, 1972. 1548.
3. *Abutalybov G.I., Belle M.L.* Semiconductors. 8, 1974. 2392.
4. *Dvornikov D.P., Salmanov V.M., Yaroshetsky I.D.* JETP Letters. 20, 1974. 17.
5. *Virko S.V., Lisitsa M.P. & Motsnyi F.V.* Phys. Solid State, 2000. 42: 1622.
6. *Belyavsky V.I. & Konchakov R.A.* Phys. Solid State, 2001. 43: 1621.
7. *Krokhmal' A.P.* Semiconductors (2003) 37: 249.
8. *Kapustyanyk V.B., Pasternak R.M., Kalush A.Z. et al.* J Appl Spectrosc, 2007. 74: 283.
9. *Segura A., Guesdon J.P., Besson J.M., Appl. Phys.* 54, 1983. 876.
10. *Alekperov O.Z., Godjaev M.O., Zarbaliev M.Z., Suleimanov R.* Sol. Stat. Comm. 77, 1991. 65.
11. *Egorov V.D., Müller G.O., Zimmermann R.* Sol. Stat. Comm. 38, 1991. 271.

STUDY OF BIOHUMUS HUMIC ACIDS EXTRACTED FROM BOTTOM SEDIMENTS

Yesenbayeva Zh.Zh.¹, Baihamurova M.O.² (Republic of Kazakhstan)

Email: Yesenbayeva432@scientifictext.ru

¹Yesenbayeva Zhanar Zhenisovna – Junior Research Associate,
SCIENTIFIC RESEARCH INSTITUTE "ECOLOGY",
KHOJA AHMET YASSAWI KAZAKH-TURKISH INTERNATIONAL UNIVERSITY;

²Baihamurova Moldir Orazaliyevna – Doctoral Student,
DEPARTMENT "ECOLOGY", FACULTY OF AGROBIOLOGY,
KAZAKH NATIONAL AGRARIAN UNIVERSITY,
ALMATY, REPUBLIC OF KAZAKHSTAN

Abstract: humic and gimatomelanoic acids are constituent components of the organic matter of the soil. Especially the possibilities of humic substances are unlimited, they find practical application in various fields of industry. The article deals with the study of biohumushumic acidsthat are extracted from bottom sediments in the Koshkorgan, Shert and Yermakozen water resevoirs of the South Kazakhstan region. As a result of research work humic acids biohumus can be used as preparations for plant growth. The high value of the biohumus obtained on the basis of bottom sediments is established. Since the bottom sediments of reservoirs are a complex multicomponent system containing both organic and mineral substances. It is shown on the basis of chemical analyzes that humic acids of Shert vermicompost have a higher density, in comparison with other samples. This shows a large amount of humic substance content.

Keywords: bottom sediment, biohumus, humic acid.

ИЗУЧЕНИЕ ГУМИНОВЫХ КИСЛОТ БИОГУМУСОВ, ПОЛУЧЕННЫХ ИЗ ДОННЫХ ОСАДКОВ

Есенбаева Ж.Ж.¹, Байхамурова М.О.² (Республика Казахстан)

¹Есенбаева Жанар Женисовна – младший научный сотрудник,
НИИ «Экология»,
Международный казахско-турецкий университет им. Ходжи Ахмеда Ясави;

²Байхамурова Молдир Оразалиевна – докторант,
кафедра экологии, факультет агробиологии,
Казахский национальный аграрный университет,
г. Алматы, Республика Казахстан

Аннотация: гуминовые и гиматомелановые кислоты являются составляющими компонентами органического вещества почвы. Возможности гуминовых веществ безграничны, они находят практическое применение в различных областях промышленности. В статье изучены гуминовые кислоты биогумусов на основе полученных из донных осадков водохранилищ (Кошкорган, Ермак-Узен, Шерт) Южно-Казахстанской области. В результате исследовательских работ гуминовые кислоты биогумусов можно использовать как препараты для роста растений. Установлена высокая удобрительная ценность полученного биогумуса на основе донных осадков. Так как донные отложения водохранилищ являются сложной многокомпонентной системой, содержащей как органические, так и минеральные вещества. Показано на основе химических анализов, что гуминовые кислоты биогумуса Шерт имеют более высокую плотность, по сравнению с другими образцами. Это показывает большие количества содержания гуминовых веществ.

Humic substances (from Latin humus - land, soil) were first isolated from peat by the Germanscientist F. Achard in 1786 and already more than 200 years are studied by scientists from different countries. Many attention to humic substances was given by the great Swedish chemist J. Berzelius.

Humic substances are responsible for the life support of soil biota and hydrobiotics, but since they remain stable for a long time (radiocarbon dating of hundreds and thousands of years), they thereby guarantee the continuous supply of plants and microorganisms with energy and building material. Humus and fulvic acid are the main components of humic substances. Humus acids are high molecular nitrogen oxycarboxylic compounds. They contain different functional groups and consist of arbitrary flavor chains, without any repetitive definite structured groups. Humus things contain mainly humic acids. They include humic acids, fulvic acids and humus. Humus acids are the group of well-soluble humus acids in the alkalis. They don't dissolve in water. There is no specific structural formula for the humus and fulvic acids. Orlov method was used to extract humic acids [1-4].

Agrochemical parameters of the soil, fertilizers are important for the growth and development of plants. Since the agrochemical parameters depend on the formation of humus and its composition (Table 1).

Table 1. Agrochemical indicators of Vermicompost (on average)

Vermicompost	Mass fraction, %				
	humus	total nitrogen	C	C:N	humic acid
Koshkorgan	6,9±0,5	4,4±0,3	14,0±0,2	4,8±0,2	4,55±0,2
Yermakozen	2,6±0,2	3,3±0,1	14,4±0,3	4,7±0,1	1,61±0,7
Shert	6,7±0,5	3,5±0,4	14,6±0,5	4,3±0,5	4,19±0,5

Optical density and radiation coefficients of humic and fulvic acids of the biohumus have been measured on the photometer "KFK-3-01" (Fig. 1, 2).

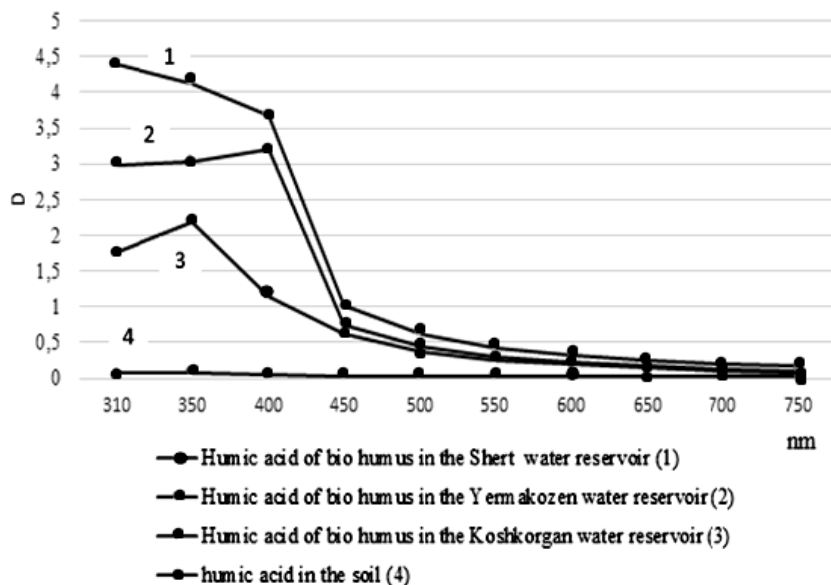


Fig. 1. Optical density of humic acid obtained from vermicompost

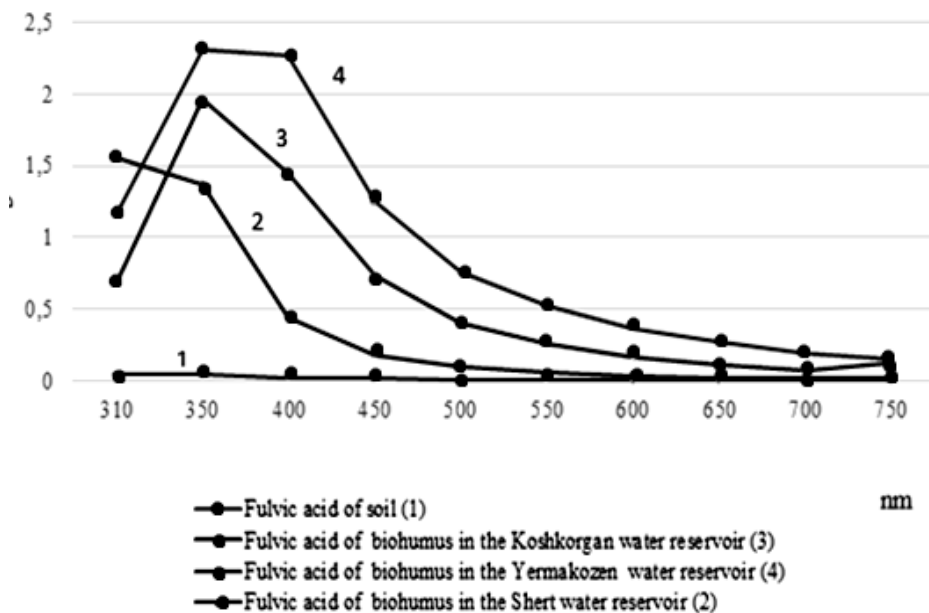


Fig. 2. Optical density of fulvic acids obtained from vermicompost

It is apparent that the value of the optical density depends on the wave length $D = f(\lambda)$ which is observed in the microwave part of the spectrum.

It was found out that the optical density of humus and fulvic acid of biohumus that obtained on the basis of bottom sediments of reservoirs is higher than the density of ordinary soil humic acid. It is characterized by the presence of aromatic humic substances. The increase in optical density can be explained by the increase of aromatic structures of molecules and the reduction of aliphatic moieties. The higher the carbon dioxide, the higher its density. The optical density of humic acids according to the above graphic schemes can be shown in the next row by Shert>Ermakozen>Koshkorgan. As it was established, various forms of humic acids impart various properties to the organism of the vermicompost in the soil system, giving them mineral substances due to their characteristics. We have also found that the microorganisms in the soil have a beneficial effect on the survival and reproduction of plants, and have a positive effect on the well-being of plants. Thus, the humus acids of biohumus obtained by treating the sludge are used in practice to increase the productivity and quality of the installation.

References in English / Список литературы на английском языке

1. Orlov D.S., Grishina L.A. Workshop on the chemistry of humus: Tutorial - Moscow: Publishing house Mosk. University, 1981. 272 p.
2. GOST R 17.4.3.07-2001 Soils. Requirements for the properties of sewage sludge in the use of fertilizers.
3. Semenov B.S. Preliminary ecological assessment of sewage sludge and soil method of their disinfection // B. Semenov, B.Z. Sytin // coll. of scientific papers. SRIAW. Moscow: Progress, 1998. P. 193-213.
4. Orlov D.S. Soil humus acids and general theory humification. Moscow: Izd-vo MGU, 1990. 325 p.

1. Орлов Д.С., Гришина Л.А. Практикум по химии гумуса // Учеб.пособие. М.: Изд-во Моск. ун-та, 1981. 272 с.
2. ГОСТ Р 17.4.3.07-2001 Почвы. Требования к свойствам осадков сточных вод при использовании их в качестве удобрений.
3. Семенов Б.С. Предварительная экологическая оценка осадка сточных вод и почвенного метода их обеззараживания // Б.С. Семенов, Б.З. Сытин // сб. научн. тр. НИИССВ. М.: Прогресс, 1998. С. 193-213.
4. Орлов Д.С. Гумусовые кислоты почв и общая теория гумификации. М.: Изд-во МГУ, 1990. 325 с.

**OPTOELECTRONIC SYSTEM FOR AUTOMATIC LANDING
OF UNMANNED SMALL AIRCRAFTS
Kulchitsky A.P.¹, Shalimov A.S.², Timoshenkov A.S.³
(Russian Federation) Email: Kulchitsky432@scientifictext.ru**

¹Kulchitsky Andrey Petrovich – Lecturer;

²Shalimov Andrey Sergeevich – PhD in Engineering Sciences, Associate Professor;

³Timoshenkov Andrey Sergeevich – Engineer,

DEPARTMENT OF MICROELECTRONICS,

INSTITUTE OF NANO- AND MICROSYSTEM TECHNOLOGY,

NATIONAL RESEARCH UNIVERSITY OF ELECTRONIC TECHNOLOGY,
MOSCOW

Abstract: a variant of constructing an opto-electronic autonomous control system based on MEMS is presented for the automatic landing of an unmanned small aircraft. The optical system for determining the bearing angles is considered using a four-quadrant photodiode. A method for calculating the bearing angles, taking into account the characteristics of the components used is given. An algorithm for automatic landing of an unmanned small aircraft with the help of an opto-electronic automated control system is considered.

Keywords: micromechanics; MEMS; gyroscope, angular velocity, navigation, orientation, unmanned aerial vehicle.

**ОПТИКО-ЭЛЕКТРОННАЯ СИСТЕМА АВТОМАТИЧЕСКОЙ
ПОСАДКИ БЕСПИЛОТНЫХ МАЛЫХ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Кульчицкий А.П.¹, Шалимов А.С.², Тимошенков А.С.³
(Российская Федерация)**

¹Кульчицкий Андрей Петрович – преподаватель;

²Шалимов Андрей Сергеевич – кандидат экономических наук, доцент;

³Тимошенков Андрей Сергеевич – инженер,

кафедра микроэлектроники,

Институт нано- и микросистемной техники,

Национальный исследовательский университет «МИЭТ»,

г. Москва

Аннотация: представлен вариант построения оптико-электронной автономной системы управления на основе МЭМС, для автоматической посадки беспилотного малого летательного аппарата. Рассмотрена оптическая система

определения углов пеленга, с использованием четырехквadrантного фотодиода. Приведен способ расчета углов пеленга, учитывающий характеристики используемых компонентов. Рассмотрен алгоритм автоматической посадки беспилотного малого летательного аппарата с помощью оптико-электронной автоматизированной системы управления.

Ключевые слова: микромеханика, МЭМС, датчик угловой скорости, угловая скорость, навигация, ориентация, беспилотный летательный аппарат.

УДК [531.768+62.752.4]:[629.1+629.7.05]

В настоящее время малые автономные подвижные объекты, такие как: роботы, беспилотные летательные аппараты самолетного и вертолетного типов, стабилизированные и вращающиеся по крену, имеют широкое применение от бытового до специального назначения и спектр применения их постоянно увеличивается. Они находят применение при решении достаточно широкого круга задач, таких как, экологический мониторинг, выявления последствий природных и техногенных катастроф, доставка малогабаритного груза, выполнение боевых задач и др. [1, 2]. Одной из стадий полета МЛА является посадка. Посадка МЛА сложная и ответственная стадия полета. На сегодняшний день существуют много разных способов посадки беспилотных МЛА самолетного типа: посадка на парашюте, с помощью сети (для МЛА массой менее 5 кг), с помощью оператора, с использованием стационарного радиотехнического оборудования, оптико-электронного оборудования (видеокамер на основе ПЗС- и КМОП-матрицах, фотодиодных сборок) [3]. При посадках МЛА на парашюте достоинством является то, что не требуется высокой точности выхода на место приземления и взлетно-посадочной полосы (ВПП), а основной недостаток – относительно большой полезный объем занимает парашют. Использование сети возможно только при малой массы МЛА. Для радиотехнических способов требуется оборудованная стационарная ВПП и сложная электронная аппаратура на борту. При использовании видеокамер на основе ПЗС- и КМОП-матрицах достоинством является высокая точность и не требуется сложного оборудования ВПП, а недостатком является требуемая большая вычислительная мощность на борту МЛА, происходит «размытие» входного сигнала при относительно высоких угловой скорости собственного колебания.

Основные требования, которые предъявляются к данным аппаратам, это уменьшение массогабаритных размеров, трудоемкости и стоимости, увеличение полезной массы (для существующих аппаратов), времени автономной работы и точности выполнения поставленных задач, а также простота их эксплуатации. Следствием основных требований является проблема создания автоматизированной системы управления (АСУ), обеспечивающей автономное управление МЛА на всех стадиях полета [2, 3].

Создание АСУ на основе МЭМС получило широкое распространение. Преимущество МЭМС по сравнению с другими аналогичными приборами – это малые массогабаритные размеры, достаточно высокие метрологические и эксплуатационные характеристики, малое энергопотребление и низкая стоимость. Недостатками являются относительно большие составляющие шумового сигнала, случайный дрейф нуля и, для некоторых типов датчиков, значительная зависимость точностных характеристик от температуры.

Вследствие чего, целесообразно проводить интеграция АСУ на основе МЭМС с другими различными системами и сенсорами, такими как GPS, датчиками давления, дальномерами и т.д., что позволяет повысить точностные навигационные характеристики.

Рассмотрим оптико-электронную автоматизированную систему управления МЛА самолетного типа на основе МЭМС, с возможностью автоматической посадки на

взлетно-посадочную полосу. В состав АСУ входит: блок навигации и ориентации (БНО) построенный из 3 микроэлектромеханических (МЭМ) датчиков угловых скоростей (ДУС), 3-х МЭМ акселерометров, 3 МЭМ магнитометров, приемника GPS сигнала, МЭМ датчика давления, лазерного дальномера и высокоскоростного микроконтроллера; оптический индикатор-координатор (ОИК), на основе четырехсекционного фотодиода; блок обработки сигналов и управления (БОСиУ) на основе высокоскоростного вычислителя; беспроводной передатчик (БПП) предназначенный для приема/передачи (при необходимости) данных. На рисунке 1 приведена блок-схема данного АСУ, с исполнительными устройствами МЛА (ИУ), такими как рули высоты и направления, элероны, тяга двигателя.

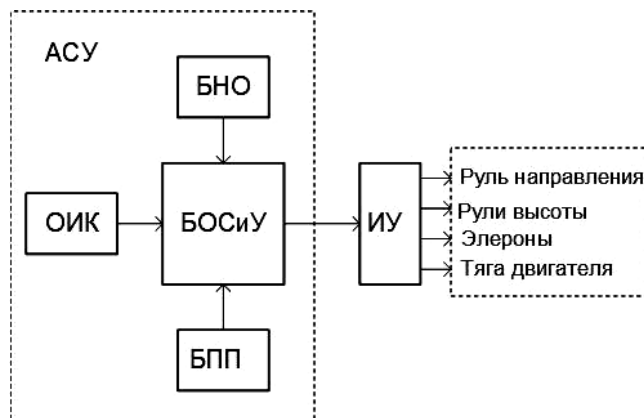


Рис. 1. Блок-схема АСУ на основе МЭМС

Автоматическая посадка БЛА по следующему алгоритму: АСУ, используя данные приемника GPS сигнала и датчика давления, выводит МЛА к месту захода на посадку, находящегося на расстоянии около 100 м от начала посадочной полосы, с точностью ± 15 м [2]. Далее, двигаясь в направлении начала посадочной полосы, БОСиУ считывает поступающие с ОИК углы пеленга маяка (маяк находится в начале посадочной полосы), а также с БНО навигационные параметры полета МЛА и, используя метод пропорциональной навигации, управляет движением МЛА в горизонтальной плоскости. Для управления МЛА в вертикальной плоскости БОСиУ использует данные поступающие с лазерного дальномера. На рисунке 2 приведена траектория движения МЛА в горизонтальной плоскости при автоматической посадке.

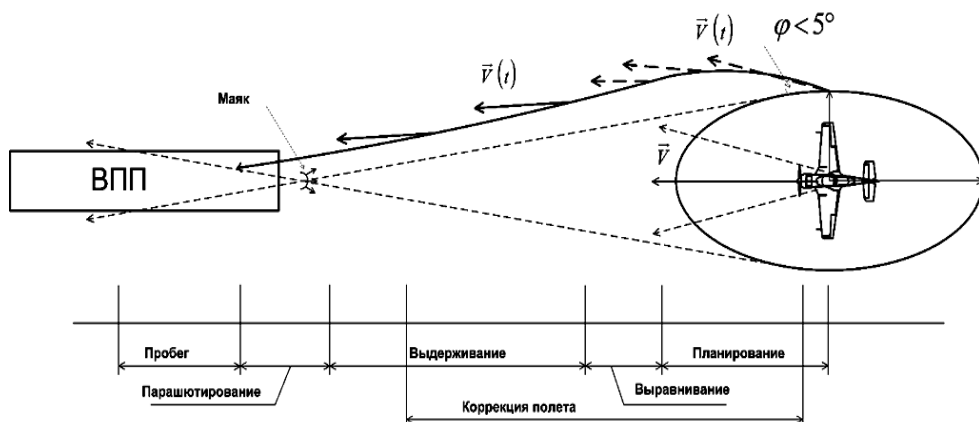


Рис. 2. Траектория движения МЛА в горизонтальной плоскости при автоматической посадке

Для создания матриц перехода из одной системы координат в другую используются кватернионы, которые не вырождаются при любом положении твердого тела (т.е. не обращаются в бесконечность ни сами параметры, ни скорости их изменения). Расчет угловой скорости поворота линии визирования и фильтрации значений проводится с помощью фильтра Калмана. Данный способ расчетов подробно рассмотрен в работах [4, 5].

Рассмотрим подробно оптический индикатор-координатор. ОИК предназначен для определения углов пеленга маяка. Разработанный ОИК имеет следующие характеристики:

- 9 ступеней автоматической регулировки сигнала (АРУ);

- диапазон плотности мощности светового пятна на входном зрачке

$$P_{\text{вх}} = (2,0 \cdot 10^{-10} \div 8,0 \cdot 10^{-8}) \text{ Вт/мм}^2;$$

- угол обзора по осям ОХ и ОУ, $\varphi_z^{\max}, \varphi_y^{\max} = \pm 20 \text{ град.};$

- среднеквадратичное отклонение (СКО) углов пеленга: на 1 ступени АРУ $\varphi_z^1, \varphi_y^1 \leq 1,5 \text{ град.}$, на 5 ступени АРУ $\varphi_z^5, \varphi_y^5 \leq 0,1 \text{ град.}$, на 9 ступени АРУ $\varphi_z^9, \varphi_y^9 \leq 0,5 \text{ град.};$

- длительность импульса – 20 мкс.

- частота поступления сигналов с маяка – 100 Гц.

В состав ОИК входят: система оптических линз; оптический фильтр с полосой пропускания длины волны от 800 нм до 1100 нм (согласованный с длиной волны излучения маяка); четырехквадрантный фотодиод (ФД); 9-ступенчатый усилитель сигнала, состоящий из операционных усилителей и усилителей с переменным коэффициентом усиления, 4 16-битных АЦП, вычислитель – микроконтроллер Cortex M3. На рисунке 3 приведена блок-схема ОИК.

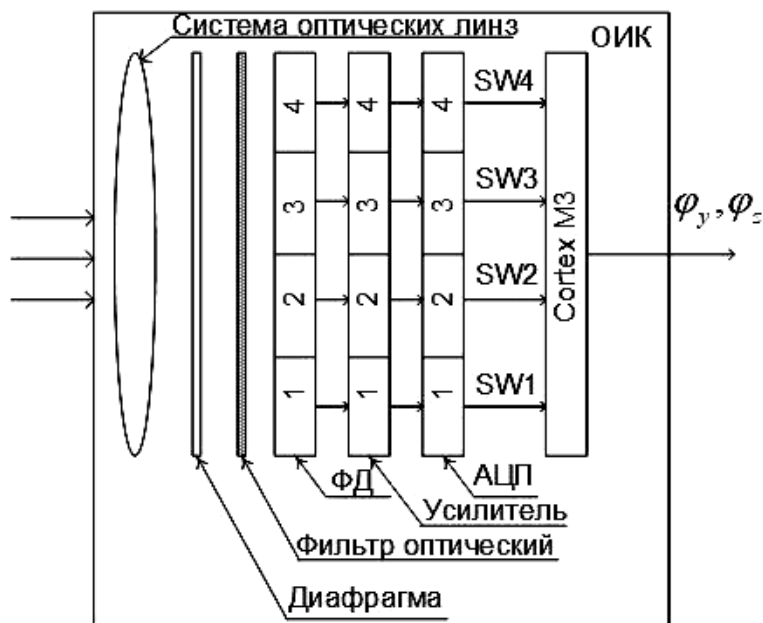


Рис. 3. Блок-схема ОИК

Принцип работы ОИК состоит в следующем: оптические сигналы, поступающие от маяка с частотой 100 Гц, проходят через систему оптических линз, диафрагму,

фильтр и попадают на 4-элементный фотоприемник в виде пятна, где преобразуются в электрический сигнал; далее, амплитуда сигнала увеличивается усилителями и с помощью АЦП преобразуется в цифровой сигнал. Вычислитель определяет истинность сигнала и рассчитывает углы пеленга φ_y и φ_z относительно системы координат ОИК и передает полученные значения в БОСиУ. На рисунке 4 показано распределение светового пятна на 4х-элементном фотоприемнике.

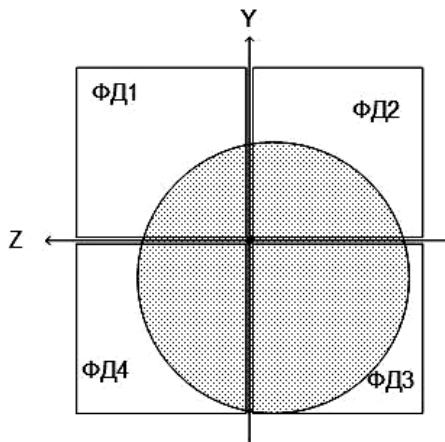


Рис. 4. Распределение светового пятна на 4-элементном фотоприемнике

Расчет углов пеленга проводятся по формулам:

$$\varphi_y = \frac{(AS_1 \cdot K_1^{AS} + AS_4 \cdot K_4^{AS}) - (AS_2 \cdot K_2^{AS} + AS_3 \cdot K_3^{AS})}{(AS_1 \cdot K_1^{AS} + AS_2 \cdot K_2^{AS} + AS_3 \cdot K_3^{AS} + AS_4 \cdot K_4^{AS})} K_0 \cdot K_y \cdot K_{\varphi y},$$

$$\varphi_z = \frac{(AS_1 \cdot K_1^{AS} + AS_2 \cdot K_2^{AS}) - (AS_3 \cdot K_3^{AS} + AS_4 \cdot K_4^{AS})}{(AS_1 \cdot K_1^{AS} + AS_2 \cdot K_2^{AS} + AS_3 \cdot K_3^{AS} + AS_4 \cdot K_4^{AS})} K_0 \cdot K_z \cdot K_{\varphi z},$$

где AS_i амплитуда оцифрованного сигнала i элемента фотодиода, K_i^{AS} – коэффициент, зависящий от характеристик фотоприемника (рассчитывается при калибровке ОИК), K_y, K_z – коэффициент, связанный с погрешностью электронных компонентов и конструкторского исполнения блока, рассчитывается при калибровке ОИК, $K_{\varphi y}, K_{\varphi z}$ – коэффициент, связанный с нелинейностью выходных данных, рассчитывается при калибровке ОИК, K_0 – коэффициент пропорциональности.

Определение истинности сигнала проводится по следующему алгоритму: по первым поступающим сигналам определяется время между ними на 1 ступени. При наличии 3 сигналов, имеющих промежуток времени между собой равной $(10 \pm 0,05)$ мс, считается, что данные сигналы истинны. Далее, во избежание ложных срабатываний, разрешение на прием сигналов выдается вычислителем через 9,95 мс, если было 2 пропущенных сигнала, то определение истинности поступления сигналов начинается заново. Далее идет определение ступени АРУ и расчет углов пеленга по двум ступеням АРУ.

Рассматриваемая оптико-электронная автоматизированная система управления МЛА самолетного типа позволяет осуществлять автоматическую посадку на площадку шириной равной 3м, грунтовая и асфальтированная автомобильные дороги

и т.д., имеет низкие энергопотребление и стоимость, относительно малый вес, а также доступность комплектующих изделий.

Представленное в настоящей работе техническое решение оптического индикатор-координатора имеет ряд преимуществ по сравнению с видеокамерами на основе ПЗС- и КМОП-матрицах – относительно низкую стоимость, малое время между поступлением сигнала и выдачи углов пеленга и может быть использовано в различных типах МЛА.

Список литературы / References

1. Цариченко С.Г., Родиченко Н.С. Беспилотные летательные аппараты, как средство повышения эффективности оперативно-тактической деятельности пожарно-спасательных подразделений // Известия ЮФУ. Технические науки, 2015. № 1. С. 14-22.
2. Пучков А.В., Алдаев С.А. Анализ навигационного оборудования, обеспечивающего посадку беспилотных летательных аппаратов // Актуальные проблемы авиации и космонавтики, 2015. Том 2. С. 970-972.
3. Соколов С.М., Богуславский А.А., Фёдоров Н.Г., Виноградов П.В. Система технического зрения для информационного обеспечения автоматической посадки и движения по ВПП летательных аппаратов // Известия ЮФУ. Технические науки, 2015. № 1. С. 96-109.
4. Тимошенков С.П., Кульчицкий А.П. Применение фильтра Калмана в системах навигации и ориентации на основе МЭМС // Оборонный комплекс – научно-техническому прогрессу России, 2013. № 1. С. 70-72.
5. Тимошенков С.П., Кульчицкий А.П. Расчет угловой скорости поворота линии визирования объекта с помощью фильтра Калмана // Оборонный комплекс – научно-техническому прогрессу России, 2014. № 2. С. 68-75.

Список литературы на английском языке / References in English

1. Carichenko S.G., Rodichenko N.C. Bepilotnye letatel'nye apparaty, kak sredstvo povyshenija jeffektivnosti operativno-takticheskoy dejatel'nosti pozharно-spasatel'nyh podrazdelenij [Unmanned aerial vehicles, as a means of increasing the effectiveness of operational and tactical activities of fire and rescue units] // Izvestija JuFU. Tehnicheskie nauki [Unmanned aerial vehicles, as a means of increasing the effectiveness of operational and tactical activities of fire and rescue units. Izvestia YuFU. Technical science], 2015. № 1. P. 14-22 [in Russian].
2. Puchkov A.V., Aldaev S.A. Analiz navigacionnogo oborudovanija, bespechivajushhego posadku bepilotnyh letatel'nyh apparatov [Analysis of navigational equipment, ensuring the landing of unmanned aerial vehicles] // Aktual'nye problemy aviicii i kosmonavtiki [Actual problems of aviation and cosmonautics], 2015. Volume 2. P. 970-972 [in Russian].
3. Sokolov S.M., Boguslavskij A.A. Fjodorov N.G., Vinogradov P.V. Sistema tehničeskogo zrenija dlja informacionnogo obespechenija avtomatičeskoj posadki i dvizhenija po VPP letatel'nyh apparatov [System of technical vision for information support of automatic landing and movement on the runway of aircraft] // Izvestija JuFU. Tehnicheskie nauki [Izvestiya SFU. Technical science], 2015. № 1. P. 96-109 [in Russian].
4. Timoshenkov S.P., Kul'chickij A.P. Primenenie fil'tra Kalmana v sistemah navigacii i orientacii na osnove MJeMS [Application of Kalman filter in navigation and orientation systems based on MEMS] // Oboronnyj kompleks – nauchno-tehničeskomu progressu Rossii [Defense complex - scientific and technical progress of Russia], 2013. № 1. P. 70-72 [in Russian].

5. Timoshenkov S.P., Kul'chickij A.P. Raschet uglovoj skorosti povorota linii vizirovaniya ob#ekta s pomoshh'ju fil'tra Kalmana [Calculation of the angular rate of rotation of the line of sight of the object with the help of the Kalman filter] // Oboronnyj kompleks – nauchno-tehnicheskomu progressu Rossii [Defense complex - scientific and technical progress of Russia], 2014. № 2. P. 68-75 [in Russian].
-

USE OF NEUROETRES FOR SOLVING CYBER SECURITY ISSUES

Nazarenko Yu.L. (Russian Federation)

Email: Nazarenko432@scientifictext.ru

*Nazarenko Yuri Leonidovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON*

Abstract: the article is devoted to the review of such technology as artificial neural networks and features of using this technology. The description of the basic element of the neural network - an artificial neuron, the principles of its operation and the learning of the network as a whole is given. The features of neural networks that can be useful in solving computer security problems are described. An example of a practical problem that can be solved using artificial neural network technology is described. Examples of the successful use of neural networks in the corporate sector for solving issues of information security are given.

Keywords: cyber security, neural network, artificial neuron, threat recognition.

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ В РАМКАХ РЕШЕНИЯ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ

Назаренко Ю.Л. (Российская Федерация)

*Назаренко Юрий Леонидович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону*

Аннотация: статья посвящена обзору такой технологии, как искусственные нейросети, и особенностей использования этой технологии. Приведено описание базового элемента нейронной сети – искусственного нейрона, принципов его работы и обучения сети в целом. Описаны особенности нейросетей, которые могут быть полезны при решении проблем компьютерной безопасности. Описан пример практической задачи, которую можно решить с использованием технологии искусственной нейросети. Приведены примеры успешного использования нейросетей в корпоративном секторе для решения вопросов информационной безопасности.

Ключевые слова: кибербезопасность, нейронная сеть, искусственный нейрон, распознавание угроз.

Введение. В настоящее время компьютерные сети представляют собой большие распределенные системы программ и устройств, взаимодействующие между собой, чтобы обмениваться информацией, а также хранить ее и обрабатывать. Сети объединяют различные типы устройств, соединенных каналами связи. Усиленная нагрузка сетей, их усложнение, участвовавшееся появления методов нарушения работы, создают необходимость серьезного отношения к проблемам сетевой безопасности.

Большинство существующих систем обнаружения атак (СОА), применяемых для мониторинга безопасности информационных систем (ИС), основаны на

использовании правил и сигнатур, с помощью которых анализируется вектор входных данных и на основании чего делается вывод о наличии или отсутствии атаки. При малейшем отклонении сигнатуры атаки от сигнатуры или правила, имеющегося в БД, эта атака обнаружена не будет. Поэтому из-за большого разнообразия атак обычные СОА не всегда способны обеспечить идентификации атаки. Одним из вариантов решения этой проблемы может быть использование нейросетей.

Принципы работы нейросети. Под искусственными нейронными сетями (НС) понимают совокупность моделей биологических нейронных сетей. Структурно НС представляют собой сеть элементов - искусственных нейронов, связанных между собой синоптическими соединениями. НС обрабатывает входную информацию и в процессе изменения своего состояния во времени формирует совокупность выходных сигналов [1].

Каждый нейрон характеризуется своим текущим состоянием по аналогии с нервными клетками головного мозга, которые могут быть возбуждены или заторможены. Он обладает группой синапсов – однонаправленных входных связей, соединенных с выходами других нейронов, а также имеет аксон – выходную связь данного нейрона, с которой сигнал (возбуждения или торможения) поступает на синапсы следующих нейронов. Общий вид нейрона приведен на рис. 1.

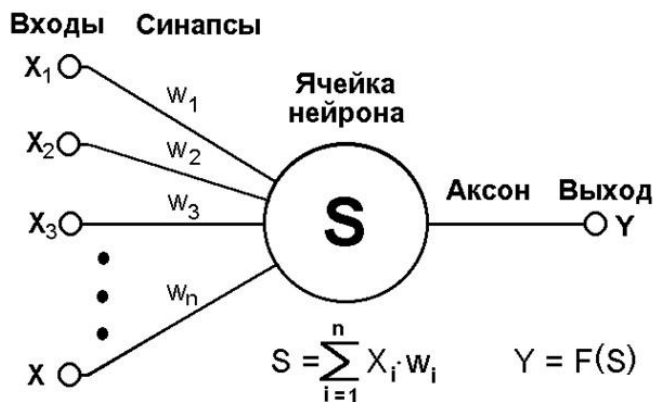


Рис. 1. Общий вид нейрона

Для НС вводится функция, определяющая порог срабатывания $Y = F(S)$

В настоящее время чаще всего используют многослойные архитектуры нейронных сетей. Обычно такая сеть состоит из входного слоя, одного или нескольких скрытых слоев и выходного слоя. Многослойная сеть изображена на рис. 2.

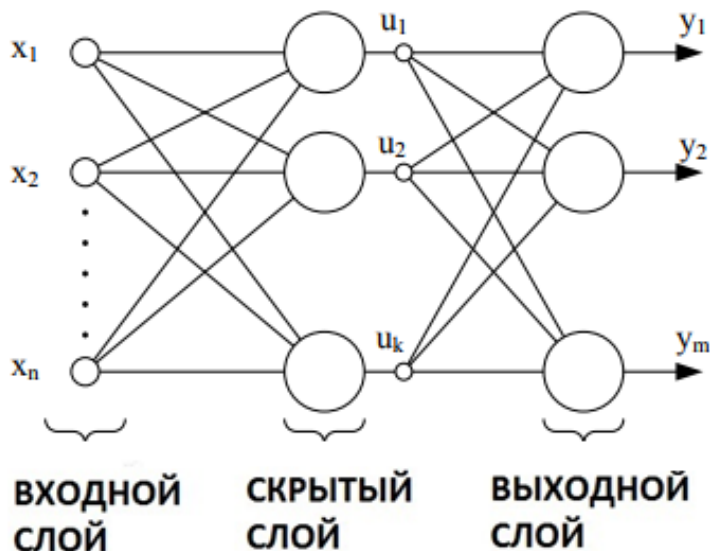


Рис. 2. Многослойная нейросеть

Можно выделить следующие наиболее распространенные архитектуры НС:

- сети прямого распространения, в которых все связи НС направлены строго от входного слоя к выходному;
- сети обратного распространения, когда сигнал может передаваться обратно к входному слою;
- сеть Кохонена – сеть с определенным слоем (слой Кохонена), таким, что сигналы этого слоя обрабатываются по правилу «победитель забирает всё», причем, наибольшему сигналу присваивается единица, а остальные сигналы обращаются в ноль [2].

Выбор структуры НС осуществляется в соответствии с особенностями и сложностью задачи.

Применение нейросетей в компьютерной безопасности.

Применение НС для решения любой задачи включает два этапа: этап обучения и этап распознавания. На этапе обучения на вход НС подается обучающая выборка, состоящая из заранее отобранных и подготовленных входных и выходных векторов [3]. В соответствии с выбранным алгоритмом обучения происходит настройка весовых коэффициентов, в результате которой при подаче на вход НС обучающего вектора на выходе появляется заданный выходной вектор, обозначающий класс входного вектора.

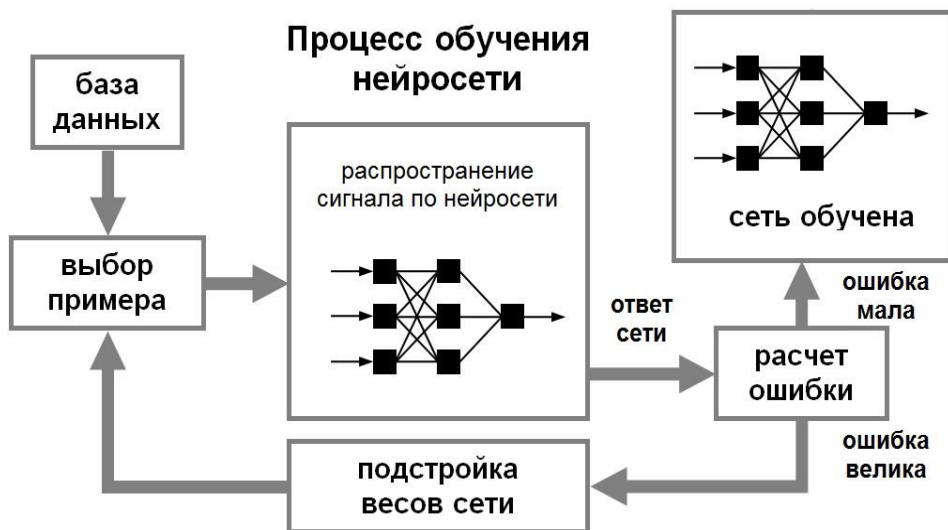


Рис. 3. Обучение нейронной сети

На этапе распознавания на НС поступает заранее неизвестный входной вектор. При этом на выходе появляется вектор – результат распознавания, в соответствии с которым входной вектор причисляется к одному из известных классов.

Наиболее важное достоинство нейронных сетей при обнаружении злоупотреблений – их способность изучать характеристики умышленных атак и идентифицировать элементы, не похожие на наблюдавшиеся в сети прежде.

После того как нейронная сеть обучена множеством последовательных команд защищаемой системы или одной из ее подсистем, сеть представляет собой «образ» нормального поведения. Процесс обнаружения аномалий представляет собой определение показателя неправильно предсказанных команд, то есть фактически обнаруживается отличие в поведение объекта.

Классификация решаемых задач в области данного метода ИИ:

- Быстрое распознавание угроз;
- Борьба с вредоносным ПО, которое так же является самообучающимся.
- Вынесение определенных сведений в процессе обучения, и построение на их основе более мощной системы защиты.

В прикладных задачах информационной безопасности нейронные сети применяются в:

- Система обнаружения атак. Сложившийся образ нормального поведения сети позволяет с высокой степенью эффективности находить и распознавать опасные аномалии.
- Межсетевых экранах. Подобно экспертной системе, нейронная проводит анализ трафика и выстраивает предположение о возможном вторжении. Плюсом нейронной сети в данном случае является ее способность самостоятельно обучаться, а не зависеть от данных, которые были заложены в нее человеком.

Использование нейросети на примере практической задачи.

В данном примере при помощи НС необходимо детектировать доступ к базе данных со стороны некоего ПО, отличного от автоматизированного рабочего места (АРМ) пользователя, или определить аномалии в работе пользователя. НС имеет четыре входа, на которые подаются:

1. Объем информации (килобайт), загружаемой из базы данных за контрольный период. Полученное значение необходимо нормализовать, поскольку считываемый из базы данных объем заранее не известен и индивидуален для каждой задачи и для каждого пользователя. В качестве нормализации можно применить оценку трафика по десятибалльной шкале (0 – объем равен нулю, 10 – максимальный объем трафика).

2. Количество транзакций в минуту.

3. Количество операций модификации данных в минуту. В этом примере АРМ использует «короткие транзакции», то есть в рамках одной транзакции обычно бывает 1–2 операции модификации данных.

4. Признаки обращения к словарю базы данных. Признаки будут дискретными (0 – нет обращений, 1 – есть), и их будет несколько – по одному на каждую из таблиц словаря базы.

Выход НС может быть интерпретирован как процентное соответствие текущих действий действиям хакера.

Таким же способом можно организовать определение различных атак и адаптацию к новым типам угроз.

Примеры использования нейронных сетей в целях обеспечения безопасности в корпоративном секторе.

Компания HNC Software Inc. разработала ПО Falcon, позволяющее выявлять и предотвращать широкий спектр мошеннических операций с банковскими картами. Система Falcon использует технологию поддержки принятия решения, комбинирующую расширенную БД правил обработки транзакций, статистический анализ и ИНС.

Семейство систем PRISM (компания Nestor) основано на использовании ИНС, экспертных систем и статистических методов для обнаружения мошенничества с кредитными и дебетовыми картами, а также при осуществлении финансовых или торговых сделок [4]. Особый интерес в целях обеспечения безопасности вызывают решения, связанные с распознаванием образов в системах видеонаблюдения.

Учитывая высокие темпы роста объемов накопленной в современных хранилищах данных информации, роль ИНС трудно переоценить. По мнению специалистов, интеллектуальный анализ данных войдет в десятку важнейших информационных технологий.

Список литературы / References

1. *Заенцев И.В.* Нейронные сети: основные модели // Учебное пособие к курсу «Нейронные сети».
2. Нейронная сеть Кохонена // Википедия, 2017. [Электронный ресурс]. Режим доступа: <http://ru.wikipedia.org/?oldid=88657008/> (дата обращения: 29.10.2017).
3. *Котельников Е.В., Колеватов В.Ю.* Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей. // Научная статья. Вятский государственный университет.
4. *Писаренко И.Б.* Нейросетевые технологии в безопасности // Журнал «Информационная безопасность». № 4, 2009.

Список литературы на английском языке / References in English

1. *Zaentsev I.* Neural networks: basic models // A manual for the course "Neural networks".
2. Kohonen's neural network // Wikipedia, 2017. Retrieved October 29, 2017. [Electronic resource]. URL: <http://en.wikipedia.org/?oldid=88657008>.
3. *Kotelnikov E., Kolevatov V.* Methods of artificial intelligence in the tasks of ensuring the safety of computer networks. // Scientific article. Vyatka State University.

CRYPTO STABILITY OF GENERATORS OF RANDOM NUMBERS. YARROW ALGORITHM

Nazarenko Yu.L. (Russian Federation)

Email: Nazarenko432@scientifictext.ru

*Nazarenko Yury Leonidovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON*

Abstract: the article is devoted to the technologies of realizing random and pseudo-random number generators, as well as their cryptographic stability. The main requirements for pseudo-random number generators for their use in cryptographic protocols are given. Examples of the use of cryptographic persistent pseudo-random number generators in web security are described. Possible ways of implementing random number generators are given. Separately, a concrete implementation of a cryptographically stable generator based on the Yarrow algorithm is considered, its merits and drawbacks are considered, conclusions are made about the possibility of its practical use.

Keywords: a pseudo-random number generator, cryptographic stability, the Yarrow algorithm, the mechanism of copying.

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ. АЛГОРИТМ ЯРРОУ Назаренко Ю.Л. (Российская Федерация)

*Назаренко Юрий Леонидович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону*

Аннотация: статья посвящена технологиям реализации генераторов случайных и псевдослучайных чисел, а также их криптографической стойкости. Приведены основные требования, предъявляемые к генераторам псевдослучайных чисел для их использования в криптографических протоколах. Описаны примеры использования криптографически стойких генераторов псевдослучайных чисел в веб-безопасности. Приведены возможные способы реализации генераторов случайных чисел. Отдельно рассмотрена конкретная реализация криптографически стойкого генератора на основе алгоритма Ярроу, рассмотрены его достоинства и недостатки, сделаны выводы о возможности его практического использования.

Ключевые слова: генератор псевдослучайных чисел, криптографическая стойкость, алгоритм Ярроу, механизм пересева.

Случайные числа и генераторы случайных и псевдослучайных чисел. Известно, что при реализации криптографических преобразований, используют различные случайные первичные состояния либо целые последовательности. Отсюда следует, что стойкость криптопреобразования напрямую зависит от алгоритма формирования случайных чисел и последовательностей, точнее от их степени случайности. Современные компиляторы обладают собственной реализацией

генератора псевдослучайных последовательностей, однако с криптографической точки зрения они являются непригодными [1].

Основная сложность генерации последовательности псевдослучайных чисел на компьютере в том, что компьютеры детерминистичны по своей сути. Компьютер может находиться только в конечном количестве состояний (количество состояний огромно, но конечно). Следовательно, любой датчик случайных чисел по определению периодичен. Все периодическое – предсказуемо, т.е. не случайно.

Лучшее, что может произвести компьютер – это псевдослучайная последовательность. Период такой последовательности должен быть таким, чтобы конечная последовательность разумной длины не была периодической. Относительно короткие непериодические подпоследовательности должны быть как можно более неотличимы от случайных последовательностей, в частности, соответствовать различным критериям случайности.

Генераторы случайных чисел — ключевая часть веб-безопасности. Небольшой список применений:

- Генераторы сессий (PHPSESSID)
- Шифрование
- Генерация соли для хранения паролей в необратимом виде
- Генератор паролей
- Порядок раздачи карт в интернет казино
- многое другое.

При этом ГПСЧ не лишены уязвимостей, использование которых злоумышленниками может привести к нарушению безопасности при работе с криптографическими протоколами, основанными на случайных числах (большинство является таковыми). Основными уязвимостями ГПСЧ являются:

- Предсказуемая зависимость между числами.
- Предсказуемое начальное значение генератора.
- Малая длина периода генерируемой последовательности случайных чисел, после которой генератор заикливается.

Криптографически стойкие генераторы случайных чисел. Требования к обычному генератору псевдослучайных чисел выполняются и криптографически стойким ГПСЧ, обратное неверно. Требования к КСГПСЧ можно разделить на две группы: во-первых, они должны проходить статистические тесты на случайность; а во-вторых, они должны сохранять непредсказуемость, даже если часть их исходного или текущего состояния становится известна криптоаналитику [2].

В идеале случайные числа должны основываться на настоящем физическом источнике случайной информации, которую невозможно предсказать. Примеры таких источников включают шумящие полупроводниковые приборы, младшие биты оцифрованного звука, интервалы между прерываниями устройств или нажатиями клавиш. Полученный от физического источника шум затем «дистиллируется» криптографической хэш-функцией так, чтобы каждый бит зависел от каждого бита. Достаточно часто для хранения случайной информации используется довольно большой пул (несколько тысяч бит) и каждый бит пула делается зависимым от каждого бита шумовой информации и каждого другого бита пула криптографически надежным (strong) способом.

Требования [2] к обычному генератору псевдослучайных чисел выполняются и криптографически стойким ГПСЧ, обратное неверно. Требования к КСГПСЧ можно разделить на две группы: во-первых, они должны проходить статистические тесты на случайность; а во-вторых, они должны сохранять непредсказуемость, даже если часть их исходного или текущего состояния становится известна криптоаналитику. А именно:

- КСГПСЧ должен удовлетворять «тесту на следующий бит». Смысл теста в

следующем: не должно существовать полиномиального алгоритма, который, зная первые k битов случайной последовательности, сможет предсказать $(k+1)$ -й бит с вероятностью более 50%.

• КСГПСЧ должен оставаться надёжным даже в случае, когда часть или все его состояния стали известны (или были корректно вычислены). Это значит, что не должно быть возможности получить случайную последовательность, созданную генератором, предшествующую получению этого знания криптоаналитиком. Кроме того, если во время работы используется дополнительная энтропия, попытка использовать знание о входных данных должна быть вычислительно невозможна.

Существует три класса реализации КСГПСЧ:

- На основе криптографических алгоритмов
- На основе вычислительно сложных математических задач
- Специальные реализации

Одним из КСГПСЧ, разработанных в рамках специальной реализации, является алгоритм Ярроу. Он описан в следующей части данной статьи.

Алгоритм Ярроу. Алгоритм криптографически стойкого генератора псевдослучайных чисел. В качестве названия выбран тысячелистник, засушенные стебли которого служат источником энтропии при гадании. Алгоритм разработан в августе 1999 года Брюсом Шнайером, Джоном Келси и Нилсом Фергусом из компании Counterpane Internet Security [3].

Компоненты Yarrow. Yarrow это криптографически стойкий генератор псевдослучайных чисел. Он состоит из четырёх основных компонентов:

- 1) Аккумулятора энтропии, который собирает семплы из источников энтропии в два пула (быстрый и медленный).
- 2) Механизма пересева (усложнения), периодически пересевающего ключ новой энтропией из пулов.
- 3) Механизма генерации, выполняющего генерацию псевдослучайной последовательности из ключа.
- 4) Управления пересевом, определяющего, когда нужно пересевать ключ.

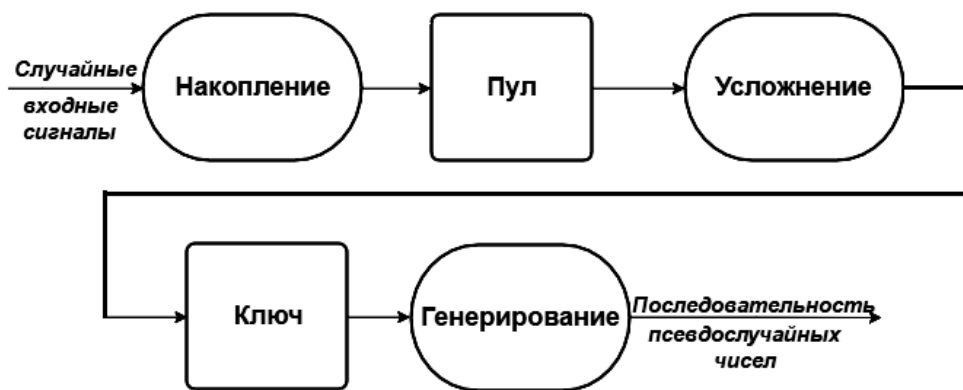


Рис. 1. Общий вид алгоритма

Аккумулятор энтропии. Аккумулятор энтропии состоит из двух пулов:

- 1) Быстрый пул (fast pool) обеспечивает частые пересевы ключа.
- 2) Медленный пул (slow pool) обеспечивает редкие, но очень консервативные (по оценке имеющейся в нём энтропии) пересевы ключа.

Каждый из пулов представляет собой текущее значение односторонней хеш-функции, на вход которой подаются семплы, содержащие энтропию. Хеш-функция

выполняет роль сборщика энтропии. Семплы из источников поочерёдно поступают то в быстрый то в медленный пул.

Измерение энтропии. Для каждого источника пул поддерживает оценку полученной энтропии в битах. Измерение энтропии весьма непростой процесс, однако практически предлагается использовать три способа:

1) Значение энтропии каждого семпла передаётся программистом в виде коэффициента.

2) Для каждого источника постоянно выдаётся оценка энтропии через специализированный определитель.

3) Общесистемный лимит, константа (0,5 в Yarrow).

Для оценки энтропии каждого семпла используется наименьший из них.

Механизм пересева. Механизм пересева соединяет аккумулятор энтропии и механизм генерации. Когда механизм пересева определяет, что нужно осуществить пересев ключа, компонента пересева должна обновить ключ, используемый механизмом генерации, из одного или двух пулов. Осуществить это нужно так, что если атакованному был известен или ключ или содержимое пулов, то ключ пересева остался ему неизвестным.

Управление пересевом. Частый пересев желателен, но потенциально повышает вероятность успеха итерационной атаки. Редкий пересев оставляет больше информации атакованному, получившему ключ. Дизайн управления пересевом должен быть компромиссным между этими двумя взаимно противоречивыми требованиями.

Механизм генерации.

Используются 2 алгоритма:

Односторонняя хеш-функция $h(x)$, с отпечатком размером m -бит, которая должна обладать следующими свойствами:

- быть необратимой, то есть стойкой к восстановлению прообраза;
- быть стойкой к коллизиям;
- давать на выходе m -бит.

В Яроу-160 используется алгоритм SHA-1 в качестве $h()$.

Блочный шифр $E_K()$ с ключом длиной k -бит и n -битным блоком [4].

- иметь ключ длиной k -бит и блок данных размером n -бит;
- быть устойчивым к открытому тексту и атакам по выбранному тексту;
- иметь хорошие статистические свойства выходных сигналов, даже при высокошаблонных входных сигналах.

В Яроу-160 используется алгоритм 3-KEY Triple DES в качестве $E_K()$.

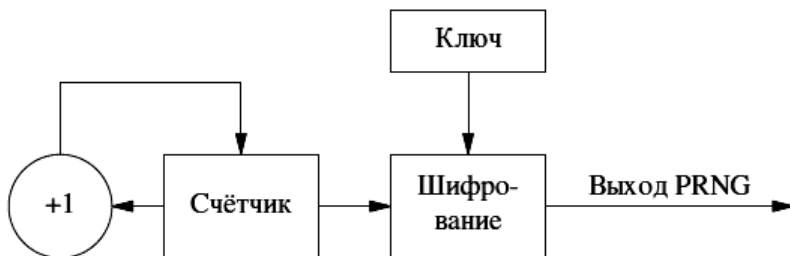


Рис. 2. Механизм генерации

Для генерации следующих n -бит псевдослучайной последовательности счётчик C увеличивается на 1 и зашифровывается блочным шифром, используя ключ K :

$$C \leftarrow C + 1 \bmod 2^n$$

$$R \leftarrow E_K(C)$$

где R — выход псевдослучайной последовательности, а K — текущий ключ.

Если в какой-то момент ключ оказался скомпрометирован, нужно предотвратить утечку предыдущих выходных значений, которые атакующий может получить. Описанный механизм не имеет такой защиты от утечки, поэтому дополнительно ведётся подсчёт количества блоков псевдослучайных последовательностей, выданных на выход. Как только будет достигнут некий лимит $1 \leq P_g \leq 2^{n/3}$, генерируется k -битовый выход и устанавливается как ключ.

$K \leftarrow$ следующие k бит выхода PRNG

Следует выбирать весьма консервативное значение P_g , в Yagow оно задано как 10.

Механизм пересева. Механизм пересева генерирует новый ключ K для генератора из энтропии, собранной в аккумуляторе энтропии, и существующего ключа. Время выполнения механизма пересева зависит от параметра $P_t \geq 0$.

Механизм пересева состоит из следующих шагов:

1. Аккумулятор энтропии вычисляет хеш всех входов в быстрый пул. Результат этого вычисления назовём v_0 .
2. Установить $v_i = h(v_{i-1} \| v_0 \| i)$, для $i = 1..t$
3. Установить $K \leftarrow h'(h(v_{p_i} \| K), k)$.
4. Установить $C \leftarrow E_K(0)$
5. Сбросить все счётчики энтропии в пулах в 0.
6. Очистить всю память, задействованную под хранение промежуточных значений.

Достоинства алгоритма. Алгоритм был изначально спроектирован с целью достижения максимальной эффективности работы, поэтому создатели заострили внимание на следующих аспектах:

Быстрота и эффективность. Никто из разработчиков не будет использовать алгоритм, сильно замедляющий приложение.

Простота. Любой программист без особых знаний в криптографии должен суметь его безопасно использовать.

Оптимизация. Там, где это возможно, алгоритм должен использовать уже существующие блоки команд.

Недостатки алгоритма. По мнению создателей Ярроу-160, алгоритм может быть уязвим из-за плохих оценок энтропии, так как в сегодняшней реализации алгоритма Ярроу-160 размер пулов накопления энтропии ограничивается 160 битами.

Направление развития. В планах на будущее у создателей использование нового стандарта блочного шифра AES. Новый блочный шифр легко сможет разместиться в базовой конструкции алгоритма Ярроу. Для этого будет необходимо или изменить хеш-функцию усложнения, или разработать новую хеш-функцию, чтобы обеспечить заполнение пула энтропии более чем 160 битами. Для AES со 128 битами это не будет проблемой, а для AES со 192 или 256 битами эту проблему придется разрешить.

Набор правил для механизма управления усложнением по-прежнему остается временным. По этой причине это является предметом постоянных исследований.

Выводы. В настоящее время алгоритм Ярроу является сильно защищенным генератором псевдослучайных чисел. Это позволяет использовать его для широкого спектра задач: шифрования, электронной подписи, целостности информации и других задач.

Список литературы / References

1. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ, 2002.
2. Алгоритм Yagow — краткий обзор Ситкарев Г.А. Сыктывкарский государственный университет. Лаборатория программирования и прикладной математики.

3. *Шнайер Б.* Генерация случайных и псевдослучайных последовательностей // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си— М.: Триумф, 2002. 816 с.
4. Алгоритм Яроу // Википедия. [Электронный ресурс]. Режим доступа: <http://ru.wikipedia.org/?oldid=85118712/> (дата обращения: 29.04.2017).

Список литературы на английском языке / References in English

1. Cryptographic protection of information in information systems. Lecture course. Gorbenko I. KNUR, 2002.
 2. The Yarrow algorithm is an overview. Sitkarev G.A. Syktyvkar State University Laboratory of Programming and Applied Mathematics.
 3. *Schneier B.* Applied Cryptography. Protocols, Algorithms and Source Code in C., 2002. 816 p.
 4. Yarrow algorithm. (2017. September, 12). In Wikipedia. The Free Encyclopedia. Retrieved 22:46, December 7, 2017. [Electronic resource]. URL: <https://en.wikipedia.org/w/?oldid=800273269/> (date of access: 29.04.2017).
-

CRYPTOANALYSIS OF CIPHER OF SIMPLE REPLACEMENT

Sinochkin D.V. (Russian Federation)

Email: Sinochkin432@scientifictext.ru

Sinochkin Denis Vadimovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON

Abstract: this article is devoted to the method of hacking the cipher of Caesar with the keyword. Describes the main goals and the need for encryption of information, as well as a method of hacking absolutely any code. An example is given of one of the possible variants of hacking the cipher of a simple substitution with the help of a proximity measure, a proximity matrix of an open text, and frequency characteristics of the plaintext. An example of cryptanalysis of cipher text is given regardless of the length of the key. The dependence of the decryption efficiency on the key length is determined.

Keywords: cryptanalysis, encryption, simple replacement code, frequency characteristics.

КРИПТОАНАЛИЗ ШИФРА ПРОСТОЙ ЗАМЕНЫ

Синочкин Д.В. (Российская Федерация)

Синочкин Денис Вадимович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону

Аннотация: данная статья посвящена методу взлома шифра Цезаря с ключевым словом. Описаны основные цели и необходимость шифрования информации, а также рассмотрен метод взлома абсолютно любого шифра. Приведен в пример один из возможных вариантов взлома шифра простой замены с помощью меры близости, матрицы близости открытого текста, а также частотные характеристики открытого текста. Приведен пример криптоанализа шифротекста вне зависимости от длины ключа. Определена зависимость эффективности дешифровки от длины ключа.

Ключевые слова: криптоанализ, шифрование, шифр простой замены, частотные характеристики.

Введение. В настоящий момент существует огромное количество методов шифрования. Главным образом эти методы делятся на симметричные и асимметричные методы, но секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования известен только доверенным лицам. Ключ – важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для шифрования конкретного сообщения [1]. В современном мире криптография находит множество различных применений: для передачи информации, она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi и на транспорте для защиты билетов от подделок, и в банковских операциях, для электронного документооборота.

Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам – криптоанализу [2].

Анализ необходимости шифрования данных. Современные криптографические системы позволяют расшифровать информацию по различным типам алгоритмов буквально в доли секунды. Уровень развития информационных технологий позволяет добиться высокого уровня шифрования, но и при этом дешифрование так же не остается на месте. Несмотря на защищенность каналов связи, информация может быть перехвачена

непосредственно на принимающем устройстве. После этого, если она не была зашифрована должным образом, будет расшифрована злоумышленниками и будет нанесен вред необходимому для него объекту [3].

Современные алгоритмы шифрования разрабатываются таким образом, чтобы аналитик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные. Любая система шифрования, кроме абсолютно криптостойких, может быть взломана простым перебором всех возможных ключей. Но перебирать придётся до тех пор, пока не отыщется тот единственный ключ, который и поможет расшифровать шифротекст, то есть необходимо перебрать $n!$ ключей, однако ей сложно выделить правильный текст. Невозможность взлома полным перебором абсолютно криптостойкого шифра так же основана на необходимости выделить в расшифрованном сообщении именно то, которое было зашифровано в криптограмме. Перебирая все возможные ключи и применяя их к абсолютно стойкой системе, криптоаналитик получит множество всех возможных сообщений, которые можно было зашифровать (в нем могут содержаться и бессмысленные сообщения).

Основные соображения взлома шифра простой замены. Любой метод вскрытия шифра простой однобуквенной замены основан на том обстоятельстве, что с точностью до переобозначений частотные характеристики m -грамм шифротекста и открытого текста одинаковы. При этом существенно используются априорные частотные характеристики предполагаемого открытого текста. Такие характеристики являются более рельефными для литературных текстов. Чем менее рельефно распределение знаков текста, тем сложнее задача вскрытия шифра простой замены. Далее будем решать задачу вскрытия простой замены лишь для литературных текстов и на статистику. Алгоритм вскрытия простой замены по тексту криптограммы достаточно тяжело формализовать. При любой попытке формализации теряется какой-нибудь важный нюанс. Поэтому укажем лишь основные идеи, лежащие в основе такого алгоритма: подсчет частот встречаемости шифрообозначений, а также некоторых их сочетаний, например, биграмм и триграмм подряд идущих знаков; выявление шифрообозначений, заменяющих гласные и согласные буквы; выдвижение гипотез о значениях шифрообозначений и их проверка. Восстановление истинного значения шифрообозначений.

Если длина текста достаточно велика, то найденные на 1 этапе частоты окажутся близкими к табулированным значениям частот знаков. Хорошим критерием является читаемость восстанавливаемого открытого текста. При проверке гипотез о значениях шифрообозначений полезен поиск в шифротексте слов с характерной структурой, которые часто встречаются в открытом тексте. Если с помощью приведенных соображений произведено несколько идентификаций шифрообозначений, то дальнейшая работа по вскрытию текста криптограммы не представляет особого труда. Однако, если известно, что использовался аффинный шифр, то существует критерий, основанный на близости матрицы биграмм

$$\Delta(t) = (\Delta_{ij}(t))_{n \times n}$$

данного текста t эталонной матрице биграмм открытого текста

$$B = (b_{ij})_{n \times n},$$

где n – число букв алфавита.

Мерой близости служит следующая целевая функция $f(t)$, связывающая матрицы $\Delta(t)$ и B :

$$f(t) = \sum_{ij} |\Delta_{ij}(t) - b_{ij}|$$

Будем исходить из того предположения, что если y – данная криптограмма и D_k – правило расшифрования на ключе k данного шифра простой замены, то для истинного ключа k_u значение

$$f(D_{k_u}(y)) = \sum_{i,j} |\Delta_{ij}(D_{k_u}(y)) - b_{ij}|$$

должно быть минимальным.

Идея основного шага алгоритма состоит в том, чтобы исходя из некоторого первичного «приближения» k для ключа k_u , основанного, например, на диаграмме частот букв, немного его изменять неким способом, уменьшая значение целевой функции $f(t)$.

Криптоанализ шифротекста. Для наиболее точного подбор ключа шифротекста необходимо проанализировать частотные характеристики данного текста и сравнить их со статистическими характеристиками русских букв в текстах. Для этого необходимо отсортировать по убыванию частоты букв статистики и шифротекста и сопоставить их в качестве начального ключа. Данный метод позволит точно расшифровать 2 - 4 символа исходного текста, что не достаточно для полной расшифровки. Поэтому необходим дополнительный алгоритм, состоящий в получении биграмм шифротекста и сопоставления их с биграммами открытого литературного текста, после чего производится подсчет меры совпадения биграмм шифротекста с биграммами открытого текста путем перестановки символом в ключе между собой. Для поиска ключа используется перестановка в нем соседних символов, через символ, через 2 символа, через 5 символов. После осуществления одной из перестановок выбирается наименьшая мера, после которой происходит поиск остальными методами до получения наименьшей меры. Алгоритм перестает работать до тех пор, пока не переберём все методы перестановок. В результате дешифруем полученным ключом текст. Данный алгоритм работает долго из-за сопоставления всех биграмм. В результате получаем наиболее «читаемый» текст с незначительными ошибками. От длины ключа зависит эффективность дешифровки: чем длиннее ключ, тем сложнее дешифровать.

Список литературы / References

1. *Алферов А.П.* Основы криптографии: учебное пособие. М.: Гелиос АРВ, 2002. 480 с.
2. *Баричев С.Г.* Основы современной криптографии. // Учебный курс. 2-е изд., испр. и доп. М.: Горячая линия - Телеком, 2002. 175 с.
3. *Рябко Б.Я.* Криптографические методы защиты информации. // Учебное пособие для вузов. 2-е изд. М.: Горячая линия - Телеком, 2012. 22 с.

Список литературы на английском языке / References in English

1. *Alferov A.P.* Fundamentals of cryptography. // Atutorial. М.: Helios ARV, 2002. 480 p.
2. *Barichev S.G.* Fundamentals of modern cryptography. // A training course, 2 ed. М.: Gorjachaja linija - Telecom, 2002. 175 p.
3. *Rjabko B.Ja.* Cryptographic methods of information protection. // Textbook manual for universities, 2 ed. М.: Gorjachaja linija - Telecom, 2012. 229 p.

MODIFICATIONS AND COMBINATION OF CODES SET BY A SIMPLE FLOAT

Sinochkin D.V. (Russian Federation)
Email: Sinochkin432@scientifictext.ru

Sinochkin Denis Vadimovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON

Abstract: this article is devoted to the consideration of methods of modification and combining of noise-immune binary block codes, set over a simple field. To achieve flexibility in the design of redundant codes, modifications or combining are resorted to. The best codes for today are obtained using the modification and combination procedure. The main goals and necessity of application of these methods in modern telecommunication systems for providing error protection are described. The necessary parameters of block codes are considered. Possible methods for improving the existing code using these methods are presented, as well as their advantages.

Keywords: simple float, block codes, code modifications, code combination.

МОДИФИКАЦИИ И КОМБИНИРОВАНИЕ КОДОВ, ЗАДАННЫХ НАД ПРОСТЫМ ПОЛЕМ

Синочкин Д.В. (Российская Федерация)

Синочкин Денис Вадимович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону

Аннотация: данная статья посвящена рассмотрению методов модификаций и комбинирования помехоустойчивых двоичных блочных кодов, заданных над простым полем. Для достижения гибкости в конструировании избыточных кодов прибегают к их модификациям или комбинированию. Наилучшие на сегодня коды получены с помощью процедуры модификации и комбинирования. Описаны основные цели и необходимость применения данных методов в современных системах телекоммуникации для обеспечения защиты от ошибок. Рассмотрены необходимые параметры блочных кодов. Приведены возможные методы по улучшению существующего кода с помощью данных методов, а также их преимущества.

Ключевые слова: простое поле, блочные коды, модификации кодов, комбинирование кодов.

Введение. Развитие теории помехоустойчивого кодирования показало, что использование любых классов кодов наталкивается на принципиальные трудности, связанные с многообразием условий их применения, а так же с экспоненциальным ростом сложности декодеров при увеличении краткости, исправляемых избыточным кодом ошибок. Для достижения гибкости в конструировании избыточных кодов прибегают к их модификациям или комбинированию. Наилучшие на сегодня коды получены с помощью процедуры модификации и комбинирования. В современных телекоммуникационных системах предъявляются достаточно высокие требования к достоверности передачи информации с вероятностью ошибки на символ не хуже 10^{-9} . Проблема кодирования неразрывно связана с развитием коммуникационных систем. Основными движущими силами, развивающими это направление, являются непрерывный рост объемов и скоростей передаваемой информации, а также необходимость повышения помехозащищенности каналов связи.

Анализ необходимости модификаций и комбинаций кодов. Одним из способов обеспечения защиты от ошибок в системах связи является применение помехоустойчивых кодов. На сегодняшний день известно большое количество кодов с хорошими корректирующими способностями. Однако существующие коды не всегда подходят для конкретных практических приложений по таким параметрам, как длина кода, размерность или минимальное кодовое расстояние. Новый код с требуемыми характеристиками можно получить на основе известного кода с помощью одного из методов модификации кодов, призванные повысить гибкость в конструировании систем связи; а благодаря некоторым способам комбинирования кодов можно получить очень сильные результаты, что подтверждается, например, появлением в 1993 г. турбо кодов. Обычно модификацией кода называют изменения, вносимые в один код, а в случае, когда новый код формируется из нескольких известных кодов, говорят о комбинировании кодов [3].

Основные параметры блочных кодов. Длина кода - n ; длина информационной последовательности или размерность кода - k ; кодовое расстояние кода - d ; поле - F_q ; число исправляемых ошибок - $t = (d_{\min} - 1) / 2$.

Помехоустойчивыми называются коды, позволяющие обнаруживать и (или) исправлять ошибки в кодовых словах, которые возникают при передаче по каналам связи. Применение помехоустойчивых кодов для повышения верности передачи данных связано с решением задач кодирования и декодирования.

Задача кодирования заключается в получении при передаче для каждой k - элементной комбинации из множества q^k соответствующего ей кодового слова длиной n из множества q^n .

Задача декодирования состоит в получении k - элементной комбинации из принятого n - разрядного кодового слова при одновременном обнаружении или исправлении ошибок [2].

Модификации блочных кодов.

- **Укорочение.** Обозначим C линейный блочный (n, k, d) код над $GF(q)$ с порождающей матрицей G и проверочной матрицей H . Пусть s целое число, $0 < s < k$. В общем случае, линейный укороченный $(n-s, k-s, d_s)$ код C_s имеет расстояние $d_s > d$. Порождающая матрица кода C_s может быть получена из матрицы G исходного кода следующим образом. Предположим, что матрица G задана в систематической форме, т.е.

$$G = (I^* | P). \quad (1).$$

Тогда $(k-s) \times (n-s)$ порождающая матрица G_s укороченного кода C_s может быть получена удалением s столбцов единичной матрицы I^* и s строк, соответствующих ненулевым элементам выбранных (удаляемых) столбцов.

- **Расширение.** В общем случае, расширение кода C означает добавление e проверочных символов. Расширенный $(n+E, k, d_{\text{ext}})$ код C_{ext} имеет минимальное расстояние $d_{\text{ext}} > d$. Расширенная проверочная $(n-k + E) \times (n + E)$ матрица получается из проверочной матрицы H кода C добавлением e строк и столбцов. Наиболее известный способ расширения кода состоит в добавлении общей проверки на четность.

- **Перфорация.** В общем случае, перфорация линейных блочных кодов состоит в удалении проверочных символов, что приводит к линейному блоковому $(n-r, k, d_r)$ коду C_r с минимальным расстоянием $d_r < d$. Скорость кода возрастает, так как размерность кода не изменяется, а избыточность (число проверок) уменьшается. Проверочная матрица H_r перфорированного кода C_r получается удалением определенных столбцов проверочной матрицы H исходного кода. Эта техника эквивалентна укорочению дуального кода. Если есть проверочная матрица кода C , то удалением любых r столбцов среди k правых столбцов матрицы H и r строк,

соответствующих ненулевым элементам выбранных для удаления столбцов, получаем $(n-k-p) \times (n-p)$ матрицу.

- Пополнение кода означает добавление кодовых слов к исходному коду. Очевидным способом выполнения этой модификации при сохранении линейности кода является добавление (линейно независимых) строк в порождающую матрицу. Построенный таким образом код C_{aug} имеет параметры $(n, k+\delta, d_{aug})$, где δ — число добавленных строк. Минимальное расстояние C_{aug} есть $d_{aug} < d$. Пусть $G = (g_0^T, \dots, g_{k-1}^T)^T$ порождающая матрица кода C , где g_i^T транспонированный вектор длины n , $0 \leq i < n$.

- Выбрасывание состоит в удалении некоторых кодовых слов из кода (из множества кодовых слов). В общем случае, это приводит к нелинейному коду. Способ, сохраняющий линейность, состоит в удалении строк порождающей матрицы G исходного кода. В результате получается код C_{exp} с параметрами $(n, k-1, d_{exp} \geq d)$.

Последовательное соединение. Одним из методов комбинирования является последовательное соединение. Рассмотрим два кода C_1 и C_2 . Тогда последовательное соединение кодов C_1 и C_2 эквивалентно поочередной передаче кодовых слов $c_1 \in C_1$ и $c_2 \in C_2$, $|C_1|C_2| = \{(c_1, c_2) : c_1 \in C_1, i=1,2\}$. Результатом последовательного соединения m линейных блочных (n_i, k_i, d_i) кодов, $i = 1, 2, \dots, m$ является (n, k, d) код с параметрами

$$n = \sum_{i=1}^m n_i, \quad k = \sum_{i=1}^m k_i, \quad d = \min\{d_i\}, \quad 1 \leq i \leq m. \quad (1), (2)$$

Обозначим G_i порождающую матрицу компонентного кода C_i , $i = 1, 2, \dots, m$. Тогда порождающая матрица последовательного соединения кодов имеет вид:

$$G = \begin{pmatrix} G_1 & & & \\ & G_2 & & \\ & & \ddots & \\ & & & G_m \end{pmatrix}. \quad (3).$$

Техника чередования кодов широко используется в системах связи, требующих разного уровня защиты от ошибок. Заметим еще, что m — кратное последовательное соединение одного и того же кода эквивалентно m — кратной повторной передаче кодового слова [1].

Конструкция Плоткина. Эта конструкция основана на двух кодах C_1 и C_2 длины $n=n_1=n_2$ и состоит в формировании кода $C = [C_1|C_1+C_2]$ с порождающей матрицей

$$G = \begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}. \quad (4).$$

Этот эффективный способ построения кодов, который позволяет, имея в качестве стартовых кодов малых длин с оптимальными или близкими к оптимальным параметрами, строить бесконечные серии кодов, с такими же хорошими параметрами. Код C имеет параметры $(2n, k_1+k_2, d)$. Минимальное кодовое расстояние кода C равно $d = \min\{2d_1, d_2\}$ [1].

На практике часто случается такое, что код не всегда подходит для конкретных практических приложений по основным его параметрам, в результате чего для получения «хорошего» и гибкого кода прибегают к его модификациям или комбинированию, благодаря чему повышается вероятность исправления ошибок в кодовых словах, возрастает скорость кода, уменьшается избыточность. Как результат, такие коды широко используют в системах связи.

Список литературы / References

1. *Прокис Дж.* Цифровая связь. М.: Радио и связь, 2000. 800 с.
2. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. 320 с.
3. *Могилевская Н.С.* Введение в теорию информации. // Учебное пособие. Ростов н/Д: Издательский центр ДГТУ, 2013. 108 с.

Список литературы на английском языке / References in English

1. *Proakis J.G.* Digital communication. M.: Radio i svjaz', 2000. 800 p.
 2. *Morelos-Zaragoza R.* The art of error correcting coding. M.: Tehnosfera, 2005. 320 p.
 3. *Mogilevskaja N.S.* Vvedenie v teoriju informacii. // Uchebnoe posobie. Rostov n/D: Izdatel'skij centr DGTU, 2013 108 p.
-

RSA CRYPTANALYSIS
Sinochkin D.V. (Russian Federation)
Email: Sinochkin432@scientifictext.ru

*Sinochkin Denis Vadimovich – Student,
DEPARTMENT OF INFORMATICS AND COMPUTER SCIENCE,
DON STATE TECHNICAL UNIVERSITY, ROSTOV-ON-DON*

Abstract: *this article is devoted to methods of cryptanalysis RSA cipher. The article describes the basic concepts used in cryptography, and also considers the very purpose of data encryption. Two main methods for hacking a cryptosystem are described: factorization and discrete logarithm, including their advantages and disadvantages. Two of the most simple RSA hacking techniques are considered, the necessary parameters for complicating cryptanalysis are indicated; the complexity of each algorithm is shown.*

Keywords: *cryptanalysis RSA, RSA, cipher, factorization, discrete logarithm.*

КРИПТОАНАЛИЗ RSA
Синочкин Д.В. (Российская Федерация)

*Синочкин Денис Вадимович – студент,
факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону*

Аннотация: *данная статья посвящена методам криптоанализа шифра RSA. В статье описаны основные понятия, используемые в криптографии, а также рассмотрена сама цель шифрования данных. Описаны два основных метода взлома криптосистемы: факторизация и дискретное логарифмирование, в том числе их преимущества и недостатки. Рассмотрены два наиболее простые в реализации метода взлома RSA, указаны необходимые параметры для того, чтобы злоумышленнику потребовалось больше времени и вычислительных ресурсов; приведена сложность каждого алгоритмов.*

Ключевые слова: *криптоанализ RSA, RSA, шифр, факторизация, дискретное логарифмирование.*

Введение. Шифрование - преобразование информации в невосприимчивый формат в целях сокрытия от неавторизованных лиц с предоставлением авторизованным пользователям доступа к ней [3, стр. 9]. Секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования известен только доверенным лицам. Ключ – важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения [2, стр. 58].

В современном мире криптография находит множество различных применений: для передачи информации, она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi и на транспорте для защиты билетов от подделок, и в банковских операциях, для электронного документооборота.

Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам – криптоанализу [2].

Цель шифрования данных. Шифрование изначально использовалось только для передачи конфиденциальной информации. Однако впоследствии шифровать информацию начали с целью её хранения в ненадёжных источниках. Шифрование информации с целью её хранения применяется и сейчас, это позволяет избежать необходимости в физически защищённом хранилище. Шифрование направлено на достижение четырех основных целей:

1. Статическая защита информации, хранящейся на жестком диске компьютера или дискетах (шифрование файлов, фрагментов файлов или всего дискового пространства), исключает или серьезно затрудняет доступ к информации лицам, не владеющим паролем (ключом), т.е. защищает данные от постороннего доступа в отсутствие владельца информации.

2. Разделение прав и контроль доступа к данным. Пользователь может владеть своими личными данными, не доступными другим пользователям.

3. Защита отправляемых (передаваемых) данных через третьи лица, в том числе по электронной почте или в рамках локальной сети.

4. Идентификация подлинности (аутентификация) и контроль целостности переданных через третьи лица документов.

Атаки на RSA. Факторизация. Факторизацией натурального числа называется его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики. В отличие от задачи распознавания простоты числа, факторизация предположительно является вычислительно сложной задачей. В настоящее время неизвестно, существует ли эффективный не квантовый алгоритм факторизации целых чисел. Однако доказательства того, что не существует решения этой задачи за полиномиальное время, также нет. Для больших чисел задача факторизации является вычислительно сложной и лежит в основе широко используемых алгоритмов.

Последние исследования показали, что решить задачу RSA может оказаться легче, чем разложить N на множители, но есть основания предполагать, что в общем случае задача RSA и задача разложения на множители имеют одинаковую сложность. Поэтому наиболее естественным способом решения задачи RSA является разложение N на множители. Самые эффективные алгоритмы факторизации принадлежат к двум категориям. Первая – время выполнения зависит от размера N , числа, которое нужно разложить на множители, а зависимость от множителя p более слабая. Вторая – время выполнения зависит от размера p . Алгоритмы из обеих категорий эффективны и имеют большое значение. Тем не менее, для атаки на RSA с конкретным значением N только некоторые из них оказываются эффективными.

Задача дискретного логарифмирования. Дискретное логарифмирование — задача обращения функции g^x в некоторой конечной мультипликативной группе G . Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны. Задача нахождения дискретного логарифма лежит в основе вычислительной теории чисел, вычислительной алгебры и имеет большое значение для криптографии с открытым ключом. Задачу дискретного логарифмирования можно сформулировать как

$$\left\{ n \in \mathbb{Z}_{>1}^+, x, y, k \in \mathbb{Z}^+, y \equiv x^k \pmod{n} \right\} \xrightarrow{\text{найти}} \{k\}. \quad (1)$$

Как известно это вычислительно трудная задача, и безопасность некоторых хорошо известных криптосистем, таких как схема обмена ключами Диффи-Хелмана-Меркла, схема Эль-Гамала, основываются на этом. Имея эффективный алгоритм дискретного логарифмирования, нарушитель может создать свой открытый текст M и использовать открытую информацию (e, N) для того, чтобы создать собственный шифротекст C , а затем с помощью алгоритма дискретного логарифмирования вычислить

$$d \equiv \log_{M^e} M \pmod{N}. \quad (2)$$

Атака методом (p-1)-алгоритмом Полларда. Простые числа p и q в системе RSA необходимо также выбирать, исходя из тех соображений, чтобы $p \pm 1$, $q \pm 1$ имели по крайней мере один простой делитель, больший 10^{20} , в противном случае p можно эффективно найти, используя (p-1)-алгоритм Полларда.

Пусть $N > 1$ составное число. Следующий алгоритм с некоторой вероятностью возвращает нетривиальный делитель N .

1. Случайно выбрать $a \in \mathbb{Z}_N$. Выбрать положительное целое $k = \text{НОК}(1, 2, \dots, B)$, для соответствующей границы B .
2. Вычислить $a_k \equiv a^k \pmod{N}$.
3. Вычислить $f = \text{НОД}(a_k - 1, N)$.
4. Если $1 < f < N$, то f – делитель N , вывести f и перейти к шагу 6.
5. Иначе перейти к шагу 2 и выбрать новое a и k .
6. Завершить алгоритм.

Сложность алгоритма составляет $O(B \log B (\log N)^2)$ [1], так что алгоритм эффективен только при малом B .

Атака малых и больших шагов. Данная задача вычислительно трудная, и безопасность некоторых хорошо известных криптосистем основываются на этом.

Алгоритм заключается в следующем:

1. Вычислить $s = \sqrt{n}$.
2. Вычислить первую последовательность S , состоящую из пар $(y a^r, r)$, $r = 1, 2, \dots, s-1$.
3. Вычислить последовательность T , состоящую из пар (a^{ts}, ts) , $t = 0, 1, \dots, s$.
4. Найти соответствие пар и вычислить $x = ts - rx$, являющееся требуемым значением d .

Алгоритму необходима таблица с $O(n)$ [1] записями. Для вычисления дискретного логарифма требуется $O(\sqrt{n} \log n)$ [1] операций и память для $O(\sqrt{n})$ [1] элементов группы. Если порядок группы будет больше 10^{40} , алгоритм станет неэффективным.

Заключение. Деятельность практически любой российской компании сегодня связана с хранением и обработкой персональных данных различных категорий, к защите которых законодательством РФ выдвигается ряд требований. Для их выполнения руководство компании, прежде всего, сталкивается с необходимостью формирования модели угроз персональным данным и разработки на ее основе системы защиты персональных данных, в состав которой должно входить средство криптографической защиты информации.

Для того чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Список литературы / References

1. Сонг Ян. Криптоанализ RSA. М.: Ижевск: НИЦ «Регулярная и хаотическая динамика», 2011. 312 с.
2. Рябко Б.Я. Криптографические методы защиты информации. // Учебное пособие для вузов, 2-е изд. М.: Горячая линия - Телеком, 2012. 229 с.
3. Алферов А.П. Основы криптографии: учебное пособие. М.: Гелиос АРВ, 2002. 480 с.

Список литературы на английском языке / References in English

1. *Song Yang*. Cryptanalytic Attacks on RSA. M.: Izhevsk: NIC «Reguljarnaja i haoticheskaja dinamika», 2011. 312 p.
2. *Rjabko B.Ja.* Cryptographic methods of information protection. // Textbook manual for universities, 2 ed. M.: Gorjachaja linija - Telecom, 2012. 229 p.
3. *Alferov A.P.* Fundamentals of cryptography. // A tutorial. M.: Helios ARV, 2002. 480 p.

THE ROLE OF MARKETING COMMUNICATIONS IN THE COMPANY

Tolmachev A.V.¹, Elagina A.S.², Byzova V.E.³ (Russian Federation)

Email: Tolmachev432@scientifictext.ru

¹Tolmachev Alexey Vasilievich – Professor, Doctor of Economics,
DEPARTMENT OF MANAGEMENT AND MARKETING;

²Elagina Anastasia Sergeevna – Student;

³Byzova Vasilisa Evgenievna – Student,
DIRECTION MANAGEMENT,
FACULTY OF ECONOMICS,
KUBAN STATE AGRARIAN UNIVERSITY,
KRASNODAR

Abstract: the article analyzes marketing communications and the role, that its play in the organization. And also it considers the mechanisms of integration of new methods for effective work in the process of company promotion taking into account modern trends. The tasks that must be observed within the company to fulfill the main modern goals of the organization are considered, and as a result, its promotion to the leading positions, and then retention of its status in the world market. The possibilities of various places for marketing communications, and, consequently, the purposes of their main activities are taken into account.

Keywords: marketing communications, company, clients, purpose, product, market, marketing, specialists.

РОЛЬ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ В КОМПАНИИ

Толмачев А.В.¹, Елагина А.С.², Бызова В.Е.³

(Российская Федерация)

¹Толмачев Алексей Васильевич - профессор, доктор экономических наук,
кафедра управления и маркетинга;

²Елагина Анастасия Сергеевна – студент;

³Бызова Василиса Евгеньевна – студент,
направление: менеджмент,
экономический факультет,

Кубанский государственный аграрный университет,
г. Краснодар

Аннотация: в статье рассматривается маркетинговые коммуникации и выполняемая ими роль в организации. А также механизмы интеграции новых методов для эффективной работы в процессе продвижения компании с учётом современных тенденций. Рассматриваются задачи, которые должны соблюдаться в рамках компании для выполнения основных современных целей организации, и как следствие продвижение её на лидирующие позиции, а далее удержание своего статуса на мировом рынке. Учитываются возможности различных мест реализации маркетинговых коммуникаций, следовательно, и целей их основной деятельности.

Ключевые слова: маркетинговые коммуникации, компания, клиенты, цель, товар, рынок, маркетинг, специалисты.

In any company, marketing communication has become indispensable in recent times. For the successful development of the company, higher-quality and efficiently established

marketing communications with partners and consumers, higher authorities and competitors are needed. The role of marketing communications is not without the designated purpose of this activity. Thus, the main goals of marketing communication in the company are: complete, reliable, adequate and current information delivery to customers and customers about goods, works and services; maximally convincing, intriguing and unobtrusive convictions of the client that visiting this particular company, store, premises for him is the most profitable option and it is very interesting and tempting; prompting the buyer to take action, i.e. obtaining information about buying, visiting, viewing advertising. To achieve these basic goals, marketing communications are used. Their role in this case is extremely important, since communication, being the process of transferring information from one object to another, has a strong incentive effect [1, p. 6].

For successful work in the market, the company must deliver its marketing messages to any places where it is possible to contact the target audience with its trademark. The places of realization of such contacts can be very different: from the store directly selling the goods, to the room in which the buyer can see commercials on TV or call a "hot" telephone line and get the information that interests him. Marketing specialists can plan in advance some types of contacts, for example, arising during the advertising campaign, but sometimes the contacts take place regardless of the plans developed. Such unplanned contacts can occur as a result of the dissemination of certain information received by customers. In particular, the general design of a trading company can unequivocally say that it trades only in inexpensive goods, and a low level of service will indicate that the firm takes little care of the interests of customers. To have the greatest effect on the target audience, the company should consider the problem of possible contacts with the consumer as an important part of its marketing program. To successfully implement the latter, it is necessary that the marketing appeal at each contact point works to convince the buyer of the merits of the proposed product [2, p. 3]. The effectiveness of advertising, holding of actions and exhibitions, the distribution of advertising leaflets, constant updating and improvement of press releases has long been proven.

The main achievement of recent years in the field of marketing communications has been the deep integration of all kinds of communication with clients in various forms. The combination of all possible means and methods of marketing communication will bring the maximum effect, allowing the company not only to fulfill its intended goals, but also to realize the mission chosen in its field of activity. Communication of a marketing nature is especially important today, when the political, economic and social spheres undergo daily changes. Qualitative, competently prepared and implemented marketing communications is a necessary condition for the effective existence and prosperity of the company in an imminent competitive environment [3, p. 9].

References in English / Список литературы на английском языке

1. Tolmachev A.V. Upravlenie organizaciej (predprijatiem): ucheb. Posobie [Management of an organization (enterprise): textbook] / Tolmachev A.V., Ivanova I.G. Krasnodar, 2016. [in Russian].
2. Tolmachev A.V., Ivanova I.G. K voprosu podgotovki menedzherov proizvodstva. [To the issue of training production managers] // V sbornike: kachestvo sovremennyh obrazovatelnyh uslug – osnova konkurentnosposobnosti vuza sbornik statej po materialam mezhfakultetskoj uchebno-metodicheskoy konferencii [In the collection: The quality of modern educational services - the basis for the competitiveness of the university collection of articles on the materials of the inter-faculty educational and methodological conference] Responsible for the release of MV Shatalov, 2016. S. 472-474 [in Russian].

3. *Ivanova I.G., Sharapova T.N.* Filosofija upravljenja personalom organizazsii [Philosophy of personnel management of the organization.] // V sbornike: Trud i sozialno-trudovye otnoshenija: sovremennaja teorija, metodologija i praktika sbornik nauchnyh trudov po materialam I mezhdunarodnoj nauchno-prakticheskoy konferencii [In the collection: Labor and Social and Labor Relations: Modern Theory, Methodology and Practice, a collection of scientific papers on the basis of the I International Scientific and Practical Conference], 2016. P. 25-34 [in Russian].

References / Список литературы

1. *Толмачев А.В.* Управление организацией (предприятием): учеб. пособие / Толмачев А.В., Иванова И.Г. Краснодар, 2016.
 2. *Толмачев А.В., Иванова И.Г.* К вопросу подготовки менеджеров производства. / В сборнике: Качество современных образовательных услуг - основа конкурентоспособности вуза сборник статей по материалам межфакультетской учебно-методической конференции. Ответственный за выпуск М.В. Шаталова, 2016. С. 472-474.
 3. *Иванова И.Г., Шаранова Т.Н.* Философия управления персоналом организации. / В сборнике: Труд и социально-трудовые отношения: современная теория, методология и практика сборник научных трудов по материалам I международной научно-практической конференции, 2016. С. 25-34.
-

ANALYSIS OF THE INDEX OF BUSINESS EXPECTATIONS OF ENTREPRENEURS FROM STATE SUPPORT MEASURES

Guliev Sh.R. (Russian Federation) Email: Guliev432@scientifictext.ru

Guliev Shamil Rzaevich – Student,
INSTITUTE OF ECONOMICS AND LAW,
MOSCOW TECHNOLOGICAL UNIVERSITY, MOSCOW

Abstract: in the article the analysis of the results of the index for business expectations of small and medium-sized businesses in obtaining a variety of support measures from the state. Identify the causes of the lack of desire of entrepreneurs to use available state aid, expressed in subsidies and grants. On this basis, it is considered one of the probable reasons for the reduction in the number of individual entrepreneurs, lack of confidence in the effectiveness of existing measures become a barrier in their usage that led to the decline.

Keywords: entrepreneurs, small business, medium business, government, investment.

АНАЛИЗ ИНДЕКСА БИЗНЕС-ОЖИДАНИЙ ПРЕДПРИНИМАТЕЛЕЙ ОТ МЕР ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ

Гулиев Ш.Р. (Российская Федерация)

Гулиев Шамиль Рзаевич – студент,
Институт экономики и права,
Московский технологический университет, г. Москва

Аннотация: в статье проведен анализ результатов индекса по бизнес-ожиданиям представителей малого и среднего бизнеса в получении различных мер поддержки со стороны государства. Выявлены причины отсутствия желания у предпринимателей использовать имеющуюся государственную помощь, выраженную в субсидиях и грантах. Исходя из этого, рассмотрена одна из вероятных причин уменьшения количества индивидуальных предпринимателей, неуверенность которых в эффективности существующих мер стала преградой в их использовании, что и привело к снижению.

Ключевые слова: предприниматели, малый бизнес, средний бизнес, государство, инвестиции.

Согласно индексу RSBI (динамический индекс бизнес-ожиданий российских компаний в сегменте малого и среднего предпринимательства, базируется на фактах или мнениях и является индикатором экономической ситуации, обновляется каждый квартал), предприниматели (44%) сомневаются в эффективности государственных мер поддержки. Об этом свидетельствует опубликованное исследование бизнес-настроений владельцев малых и средних предприятий, проведенное агентством Magram Market Research, Промсвязьбанком и «Опорой России».

Для 44% опрошенных владельцев бизнеса получение консультаций, субсидий, грантов и другой помощи государства требует определенных усилий. Вероятно, именно по этой причине они крайне не уверены в эффективности таких мер — воспользовались господдержкой за последние пять лет не более 7% предпринимателей. И, по данным Индекса Опоры, чаще это крупные компании в сфере производства.

Тем не менее, по данным Индекса Опоры RSBI, предприниматели сегодня гораздо лучше осведомлены о действующих в стране программах поддержки — лишь 20% бизнесменов ничего не знают об используемых государством инструментах

стимулирования предпринимательской инициативы. Однако большинство воспринимает в качестве адресной помощи финансовые стимулы [1]. Упрощение процедуры подготовки и сдачи отчетности, снижение количества проверок являются само собой разумеющимися условиями ведения бизнеса и к заслугам государства предприниматели их не относят.

В 2013–2014 годах на поддержку малого и среднего бизнеса в общей сложности было выделено из бюджета более 135 млрд руб., включая поддержку сельхозпроизводителей, финансирование проектов Фонда содействия развитию малых форм предприятий в научно-технической сфере (Фонд Бортника) и гарантии Агентства кредитных гарантий.

По данным Минэкономразвития РФ, объемы финансирования не снижаются. В 2015 году финансирование программ господдержки малого и среднего бизнеса по линии ведомства сохранится на уровне 18,5 млрд руб. Большая часть (16,9 млрд руб.) приходится на выплату предпринимателям прямых субсидий, финансирование гарантийных фондов и микрофинансовых организаций. На объекты инфраструктуры для малого и среднего бизнеса в бюджете ведомства заложено 1,6 млрд руб.

В виде прямых субсидий предпринимателям достается порядка 10 млрд руб. Приоритет отдан бизнесу, обновляющему производство. Доля субсидий на поддержку субъектов малого и среднего предпринимательства, осуществляющих модернизацию производства товаров (работ, услуг), в том числе субсидирование процентной ставки по кредитам и субсидирование лизинга оборудования, составляет около 70% этих средств.

В Минэкономразвития отмечают, что предприятия, получившие микрозаем или поручительство гарантийного фонда, а также те, кому удалось попасть в бизнес-инкубаторы и технопарки, более стабильны. Выжить даже в кризисные времена чаще удается предприятиям, осуществляющим экспортную деятельность.

Инструменты поддержки малого и среднего предпринимательства, применяемые в России, соответствуют лучшим международным практикам развитых и развивающихся стран, таких, как США, Япония, Малайзия, Южная Африка, страны Европейского Союза. Объемы финансирования представлены в табл. 1.

Таблица 1. Бюджет на один субъект малого и среднего предпринимательства

Страна	Бюджет (руб.)
Россия	3800
США	5700
Япония	8400
Южная Африка	12203
Малайзия	115162

Список литературы / References

1. Ильин И.Е. Малый бизнес в России: проблемы и перспективы // Банковское кредитование, 2015. № 2. 33 с.
2. Круглова Н.Ю. Основы бизнеса (предпринимательства): учебник / Н.Ю. Круглова. М.: КНОРУС, 2010. 544 с.

Список литературы на английском языке / References in English

1. Ilin I.E. Malyj biznes v Rossii: problemy i perspektivy [Small business in Russia: problems and prospects] // Bankovskoe kreditovanie. [Bank lending], 2015. № 2. P. 33 [in Russian].

2. *Kruglova N.Yu. Osnovy biznesa (predprinimatel'stva): uchebnik / N.Yu. Kruglova [the Basics of business (entrepreneurship): textbook / N. Yu. Kruglov]. M.: KNORUS, 2010. P. 544 [in Russian].*

THE DEVELOPMENT INSTRUMENTS OF COMPANIES ENGAGED IN INNOVATION ACTIVITIES

Guliev Sh.R. (Russian Federation) Email: Guliev432@scientifictext.ru

*Guliev Shamil Rzaevich – Student,
INSTITUTE OF ECONOMICS AND LAW,
MOSCOW TECHNOLOGICAL UNIVERSITY, MOSCOW*

Abstract: *the article considers Russian and foreign experience on the use of measures of state support for companies. On the basis of this comparison, the proposed method of development of only those firms that are most promising and ready to work with a variety of innovative developments. These include effectively developing, fast-growing companies and innovative startups, are able to carry out R & D with investment from the state. In the example given a few successful firms that have gone through this system to support innovation.*

Keywords: *innovations, state support, business, lending, market.*

ИНСТРУМЕНТЫ РАЗВИТИЯ КОМПАНИЙ, ОСУЩЕСТВЛЯЮЩИХ ИННОВАЦИОННУЮ ДЕЯТЕЛЬНОСТЬ Гулиев Ш.Р. (Российская Федерация)

*Гулиев Шамиль Рзаевич – студент,
Институт экономики и права,
Московский технологический университет, г. Москва*

Аннотация: *в статье рассмотрен как российский, так и зарубежный опыт по использованию мер государственной поддержки компаний. На основе проведенного сравнения предложен способ развития лишь тех фирм, которые являются наиболее перспективными, готовыми работать с различными инновационными разработками. К ним можно отнести эффективно развивающиеся, быстрорастущие компании и инновационные стартапы, способные осуществлять НИОКР при вложении инвестиций со стороны государства. В пример приведены несколько успешных фирм, которые прошли через данную систему поддержки инновационной деятельности.*

Ключевые слова: *инновации, государственная поддержка, бизнес, кредитование, рынок.*

Приоритетом в настоящий момент должно быть наращивание объемов государственной поддержки и помощи развивающимся компаниям.

Например, небольшое научно-производственное объединение НПО «Стример», получившее шесть лет назад грант в рамках антикризисной программы фонда в размере 8 млн руб., выросло за это время в крупного производителя устройств молниезащиты. Доходы компании увеличились с 60 млн до 500 млн руб. в год.

«Стример» вышел на международные рынки. Даже небольшая субсидия может выступить катализатором развития при грамотно выстроенной стратегии работы проекта и правильно выбранной команде [1].

Меры господдержки должны быть достаточно гибкими, чтобы своевременно подключать лучшие мировые практики и отказываться от неэффективных

инструментов. Средства, предоставляемые предпринимателям на возвратной основе, более эффективны, чем безвозвратные субсидии [2]. Важно, чтобы стоимость этих денег была максимально доступна. Кроме того, за рубежом есть интересные механизмы косвенного стимулирования предпринимательской активности. Например, поддержка инвестиций в НИОКР за счет вычета затрат на эти цели из налогооблагаемой базы с повышающими коэффициентами.

По мнению бывшего председателя правления МСП Банка Крюкова С.П., «эффективными могут стать механизмы поддержки инновационных компаний, применяемые в Норвегии. Там разработчикам новых продуктов для крупного бизнеса компенсируется до 60% затрат на НИОКР. За десять лет реализации этой программы только 12% из 1200 профинансированных проектов оказались неудачными».

Наиболее перспективная точка приложения усилий — это поддержка быстрорастущих предприятий — так называемых «газелей». Такие компании захватывают лидерство на локальных рынках и формируют вокруг себя кластеры, в которых развиваются другие маленькие компании — поставщики, дистрибьюторы, сервисные компании.

Профессор НИУ «Высшая школа экономики» Александр Юльевич Чепуренко считает бюджетные субсидии начинающим предпринимателям неэффективным расходом бюджетных средств, утверждая: «Рост надо стимулировать в тех группах, которые имеют внутренние предпосылки роста, — это инновационные стартапы и быстрорастущие средние компании». Профессор НИУ ВШЭ также считает, что компаниям-«газелям» на государственном уровне уделяется мало внимания: «Только в прошлом году их стали упоминать в различных концептуальных документах Минэкономразвития РФ».

В 2016 году интересы малого бизнеса при принятии государственных решений будут рассматриваться в приоритетном порядке, сообщили в Минэкономразвития. Более того, малые и средние предприниматели смогут привлечь к себе людей, потерявших работу, в том числе и в крупных компаниях.

По оценке специалистов, быстрорастущих средних компаний в России менее трех сотен, но именно они ищут возможности для тиражирования бизнеса. Для них сейчас важно получать кредитные линии на длительные сроки. Если расти темпом 25–30% в год, то даже нынешние проценты по кредитам, теоретически, можно легко переносить. Необходимо стимулировать регионы, чтобы они использовали свои недостои и пустые промплощадки для имущественной поддержки таких компаний.

Список литературы / References

1. Королева А.В. Понятие и сущность финансовых инноваций // Вопросы экономических наук, 2017. № 4. С. 43.
2. Ширяева Ю.С. Некоторые подходы к оценке инновационного развития предприятия // Креативная экономика, 2017. № 8. С. 855.

Список литературы на английском языке / References in English

1. Koroleva A.V. Ponjatie i sushhnost' finansovyh innovacij [the Concept and essence of financial innovations] // Voprosy jekonomicheskikh nauk. [Problems of Economics], 2017. № 4. P. 43 [in Russian].
2. Shirjaeva Ju.S. Nekotorye podhody k ocenke innovacionnogo razvitija predpriyatija [Some approaches to the assessment of innovative development of enterprise] // Kreativnaja jekonomika. [Creative economy], 2017. № 8. S. 855 [in Russian].

THE CONCEPT AND CHARACTERISTICS OF SELF-REGULATION INSTITUTE IN RUSSIAN FEDERATION

Zharova A.G. (Russian Federation)

Email: Zharova432@scientifictext.ru

*Zharova Anastasia Galustovna – Bachelor in Jurisprudence,
LOMONOSOV MOSCOW STATE UNIVERSITY, MOSCOW*

Abstract: *this article discusses approaches to understanding institute of self-regulation in modern society, the concept of self-regulation and variations of classifications of self-regulatory organizations. The issue of «maturity» of the market participants for the successful and efficient functioning of self-regulatory organizations. Improvement of the legislative regulation of self-regulatory organizations are marked in this article. In addition, the author reveals a violation of the principle of fair competition through mandatory involvement in certain spheres of self-regulatory organizations.*

Keywords: *self-regulation, the control function, market participants, the company, delegation of authority, self-regulatory organization.*

ПОНЯТИЕ И ОСОБЕННОСТИ ИНСТИТУТА САМОРЕГУЛИРОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Жарова А.Г. (Российская Федерация)

*Жарова Анастасия Галустовна – бакалавр юриспруденции,
Московский государственный университет им. М.В. Ломоносова, г. Москва*

Аннотация: *в данной статье рассматриваются подходы к пониманию института саморегулирования в современном обществе, понятию саморегулирования и вариации классификаций саморегулируемых организаций. Поставлена проблема «зрелости» участников рынка для успешного и эффективного функционирования саморегулируемых организаций. Отмечены несовершенства законодательного регулирования деятельности саморегулируемых организаций. Помимо этого, автором выявлено нарушение принципа добросовестной конкуренции, путем императивного вовлечения в определенные сферы деятельности саморегулируемых организаций.*

Ключевые слова: *саморегулирование, контрольная функция, участники рынка, предприятие, делегация полномочий, саморегулируемые организации.*

Саморегулирование провозглашается как основным принцип демократических реформ и трансформаций, мыслится посредством наделения самостоятельности субъектов, берущих на себя ответственность за собственные действия. В широком ключе саморегулирование понимается как противопоставление внешнему регулированию. Однако, саморегулирование это в первую очередь такое понятие, которое является базовым свойством системы регулирования, которое способствует сохранению жизнеспособности права. На данный момент существует два основных подхода понимания данного термина.

Первый подход заключается в специфическом понимании саморегулирования, а именно как регулирование, которое не зависит от стороннего внешнего регулирования. Примером может служить модель рыночной экономики, когда в роли «внешнего регулятора» выступает государство. Саморегулирование здесь – это множество вариантов упорядочивания отношений хозяйствующих субъектов,

основанных на договорных отношениях, индивидуальном регулировании, саморегулируемых организациях. Иными словами, саморегулирование в рамках этого подхода выступает в качестве оппозиции к публичному регулированию.

Второй подход к пониманию саморегулирования подразумевает под собой способность объекта регулирования сохранять свойства своей системы и целостность. В этом случае саморегулирование рассматривается как свойство права, а не противопоставляется ему. Причиной саморегулирования в данном подходе можно найти в самой системе, а не во внешней среде, в силу свойства автономности.

Российский законодатель в пункте 1 статьи 2 Федерального закона от 01.12.2007 № 315-ФЗ (ред. от 03.07.2016) «О саморегулируемых организациях» определяет саморегулирование как самостоятельную и инициативную деятельность, которая осуществляется субъектами предпринимательской или профессиональной деятельности и содержанием которой являются разработка и установление стандартов и правил указанной деятельности, а также контроль за соблюдением требований указанных стандартов и правил [1]. Из данного определения можно сделать вывод о том, что саморегулирование по своей правовой природе является институтом, то есть предусматривает установление правил, регулирующих хозяйственную деятельность экономических субъектов в определенной сфере предпринимательства, а также создание механизмов, направленных на обеспечение соблюдения этих правил. Иными словами, саморегулирование реализуется посредством создания участниками рынка специальных структур и делегирования им части полномочий.

Исходя из нормы п. 1 ст. 3 Федерального закона от 01.12.2007 N 315-ФЗ «О саморегулируемых организациях», саморегулируемыми организациями признаются некоммерческие организации, созданные в целях, предусмотренных настоящим Федеральным законом и другими федеральными законами, основанные на членстве, объединяющие субъектов предпринимательской деятельности исходя из единства отрасли производства товаров (работ, услуг) или рынка произведенных товаров (работ, услуг) либо объединяющие субъектов профессиональной деятельности определенного вида[1]. Чаще всего органы саморегулирования представляют собой бизнес-ассоциации с фиксированным членством, осуществляющих свою хозяйственную деятельность в рамках установленным ими правил.

Однако не каждое бизнес сообщество является саморегулируемой организацией. Основным элементом в данном вопросе является процесс делегирования прав и полномочий, так как именно это является основой механизма управления сделками. При отсутствии у сообщества такого рода полномочий оно может считаться лишь клубом интересов, группой давления или лоббирования, но не организацией саморегулирования. Основной целью такой организации является представительство и защита интересов. Отличительными чертами саморегулируемой организации является осуществление ею следующих функций:

- Разработка правил и стандартов деловой практики;
- Мониторинг за соблюдением этих правил и стандартов;
- Выработка системы санкций за нарушение правил;
- Формирование собственной процедуры внесудебного разрешения споров между членами сообщества и потребителями. СРО образует третейские суды для разрешения споров, возникающих между членами саморегулируемой организации, а также между ними и потребителями произведенных членами саморегулируемой организации товаров;

Главной задачей саморегулируемых организаций становится объединение юридических лиц и предпринимателей, которые действуют в той или иной отрасли экономики. Такое объединение дает возможность компаниям обмениваться опытом и знаниями, самостоятельно решать многие вопросы, связанные с профессиональной деятельностью. Кроме того, к задачам СРО также относятся:

- формирование инструкций и составление правил осуществления хозяйственной деятельности;
- контроль над выполнением участниками СРО своих обязательств перед клиентами и заказчиками;
- контроль над уровнем профессиональной подготовки сотрудников компаний, входящих в саморегулируемые организации;
- формирование компенсационного фонда из взносов новых участников СРО, который в дальнейшем будет использоваться для выплаты издержек, связанных с ущербом, нанесенным ненадлежащим выполнением обязанностей компаниями-членами СРО;
- выдача допусков к работе и свидетельств, которые становятся для предприятий-участников саморегулируемых объединений весомым доказательством профессионализма и высокого качества оказываемых услуг.

Что касается классификации СРО как организаций, основанных на принципе добровольного членства, то в зависимости от особенностей законодательного закрепления можно выделить две разновидности СРО:

- саморегулируемые организации с обязательным членством, возможность создания которых прямо предусмотрена федеральным законодательством. К данной группе относятся, например, саморегулируемые организации в сфере строительства, проектирования, страхования;
- саморегулируемые организации с добровольным членством, возможность создания которых федеральным законодательством прямо не предусмотрена, но и не запрещена.

Кроме того, исходя из функций и задач СРО, представленных выше, представляется возможным классифицировать такие организации в зависимости от наличия либо отсутствия в них различного рода контрольных и распорядительных полномочий [2]. Например, существуют:

- саморегулируемые организации, которые наделяются государством полномочиями по лицензированию, некоторому контролю за участниками рынка, как, например, в сфере оценки недвижимости. Для получения возможности частному лицу или организации осуществлять оценку недвижимого имущества, необходимо состоять в специально созданных СРО, а также отвечать требованиям выбранного СРО;
- саморегулируемые организации, не наделяемые государством публичными функциями, а созданные исключительно в рамках объединения участников рынка определенной сферы для лоббирования интересов, обмена опытом.

Исходя из федеративного устройства Российской Федерации [3] и современной практики образования СРО, такие организации можно классифицировать исходя из уровня объединения ее членов:

- СРО субъектного уровня, состоящие из региональных и межрегиональных саморегулируемых организаций и объединяющие субъекты предпринимательской или профессиональной деятельности;
- СРО федерального уровня представляют собой союзы СРО, которые состоят из организаций межрегионального уровня первого уровня.

На сегодняшний день в России действуют саморегулируемые организации во многих сферах хозяйствующей деятельности: строительство, капитальный ремонт и реконструкция; архитектурно-строительное проектирование; инженерные изыскания; пожарная безопасность; арбитражное управление; аудит; экспертная оценка; рынок ценных бумаг; туристические услуги; медицина; автомобильные перевозки и другие виды деятельности.

Как уже было упомянуто выше, участие в большинстве СРО является добровольным, но для компаний, действующих в сфере строительства, проектирования и инженерных изысканий, вступление в саморегулируемые

организации, согласно законодательству, стало обязательным. Без допуска к работе, которые выдают СРО своим членам, принимать участие в тендерах и выполнять заказы в строительстве и составлении архитектурных проектов компании не имеют права.

Но если обратиться к закону «О внесении изменений в Градостроительный кодекс РФ и отдельные законодательные акты РФ», то согласно пункту 21 статьи 47, пункту 41 статьи 48, пунктам 21, 22 статьи 52, **не требуется членство в саморегулируемой организации в строительной сфере следующего вида организациям [4]:**

1) государственным и муниципальным унитарным предприятиям, в том числе государственным и муниципальным казенным предприятиям, государственным и муниципальным учреждениям в случае заключения ими договора подряда на выполнении проектных и изыскательских работ, договора строительного подряда с федеральными органами исполнительной власти, государственными корпорациями, осуществляющими нормативно-правовое регулирование в соответствующей области, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, в ведении которых они находятся, или в случае выполнения ими функций технического заказчика от имени указанных федеральных органов исполнительной власти, государственных корпораций, органов государственной власти субъектов Российской Федерации, органов местного самоуправления;

2) коммерческими организациями, доля государственных или муниципальных унитарных предприятий, государственных автономных учреждений в уставных (складочных) капиталах которых составляет более пятидесяти процентов, в случае заключения ими договоров на выполнения проектных и изыскательских работ, договоров строительного подряда с указанными предприятиями и учреждениями;

Таким образом, государство исключает участие в СРО организаций и предприятий строительной сферы с государственной долей участия в них и разделяет хозяйствующие субъекты на субъекты с государственной долей участия, давая им определенные преимущества. Таким образом, нарушается один из основных принципов функционирования рыночной экономики – принцип конкуренции.

Исходя из действующего законодательства и фактического положения дел, саморегулируемая организация занимает некое промежуточное положение между государством и предприятиями, представляя, с одной стороны, интересы российских предприятий, с другой - выполняя часть государственных функций по контролю и защите прав третьих лиц.

Институт саморегулируемой организации, являясь посредником между российскими предприятиями и государством, выполняет так же функцию «обратной связи», что крайне важно для установления доверительных отношений. При этом, данный институт предполагает исключение чрезмерного участия государства в экономической жизни предприятий. Но полноценное, свободное и эффективное функционирование такого института возможен только при осуществлении всеми участниками рынка своей профессиональной деятельности на основании принципов добросовестности и с учетом баланса частных, общественных и публичных интересов.

СРО сегодня приводит к большей активности предприятий, позволяет им более четко регулировать известные им общественные отношения, а также сокращает бюрократический аппарат государства и затраты на его содержание. Подобная «делегация полномочий» является определенной попыткой достичь золотой середины между «кейнсианством» и «монетаризмом» в вопросе о роли государства на рынке. Кроме того, саморегулируемые организации являются неким отборным этапом для успешного функционирования компании на рынке.

Список литературы / References

1. Федеральный закон от 01.12.2007 № 315-ФЗ (ред. от 03.07.2016) «О саморегулируемых организациях» // Собрание законодательства РФ, 03.12.2007. № 49. Ст. 6076.
2. *Петров Д.А.* К вопросу о публично-правовой природе деятельности членов саморегулируемых организаций // Гражданское право, 2013. № 1. С. 15-21.
3. Конституция Российской Федерации от 12 декабря 1993 г. // Российская газета, 1993. № 237.
4. Федеральный закон от 22.07.2008 № 148-ФЗ «О внесении изменений в Градостроительный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 28.07.2008. № 30 (ч. 1). Ст. 3604.
5. *Крючкова П.В.* Саморегулирование хозяйственной деятельности как альтернатива избыточному государственному регулированию. ИИФ «СПРОС» КонфОП, 2001. С. 95.

Список литературы на английском языке / References in English

1. Federalnyi zakon ot 01.12.2007 № 315-FZ (red. ot 03.07.2016) «O samoreguliruemykh organizatsiiakh» [The law on self-regulated organisations] // Sbornie zakonodatelstva RF [collected legislation of the Russian Federation]. 03.12.2007. № 49. St. 6076 [in Russian].
2. *Petrov D.A.* K voprosu o publichno-pravovoi prirode deiatelnosti chlenov samoreguliruemykh organizatsii [To the question of public-law nature of the activities of members of self-regulatory organizations] // Grazhdanskoe pravo [Civil law], 2013. № 1. P. 15-21 [in Russian].
3. Konstitutsiia Rossiiskoi Federatsii ot 12 dekabria 1993 g. [The Constitution of the Russian Federation of 12 December 1993] // Rossiiskaia gazeta [Russian paper], 1993. № 237 [in Russian].
4. Federalnyi zakon ot 22.07.2008 № 148-FZ «O vnesenii izmenenii v Gradostroitelnyi kodeks Rossiiskoi Federatsii i otdelnye zakonodatelnye akty Rossiiskoi Federatsii» [The law on amendments to the town planning code of the Russian Federation and certain legislative acts of the Russian Federation] // Sbornie zakonodatelstva RF [collected legislation of the Russian Federation], 28.07.2008. № 30 (ch. 1). St. 3604 [in Russian].
5. *Kriuchkova P.V.* Samoregulirovanie khoziaistvennoi deiatelnosti kak alternativa izbytochnomu gosudarstvennomu regulirovaniu. [Self-regulation of economic activity as an alternative to excessive government regulation]. IIF «SPROS» KonfOP, 2001. P. 95 [in Russian].

THE IMMUNE STATUS IN PATIENTS OF DUODENAL ULCER DISEASES AND THE INFLUENCE ON ITS ERADICATIONAL AND IMMUNOMODULATORY THERAPY

Suleymanov S.F. (Republic of Uzbekistan)

Email: Suleymanov432@scientifictext.ru

*Suleymanov Suleyman Fayzullayevich – PhD in Medicine, Senior Researcher,
Head of the Department,*

*DEPARTMENT OF MICROBIOLOGY, VIROLOGY, IMMUNOLOGY AND PHTHISIOLOGY,
BUKHARA STATE MEDICAL INSTITUTE,
BUKHARA, REPUBLIC OF UZBEKISTAN*

Abstract: the immunoreactivity was analyzed in 52 patients with duodenal ulcer (DU) and 36 healthy persons. The suppression of T-system and its subsets, a tension of humoral link of immunity was observed in patient. The use traditional method of treatment was not made a result to disorder of second immunodeficiency in patients with DU.

The usage of thymoptinum, the dose of which was 1,0 mg – 1,2 mg (in one course) at second group patients (n=24) with DU cured immune disorder, increased cell immunity, and had immunocorrection and eradication features.

Keywords: immune status, duodenal ulcer, T-system immunity, humoral immunity, immunotherapy.

ИММУННЫЙ СТАТУС У БОЛЬНЫХ ЯЗВЕННОЙ БОЛЕЗНЬЮ ДВЕНАДЦАТИПЕРСТНОЙ КИШКИ И ВЛИЯНИЕ НА НЕЁ ЭРАДИКАЦИОННОЙ И ИММУНОМОДУЛИРУЮЩЕЙ ТЕРАПИИ Сулейманов С.Ф. (Республика Узбекистан)

*Сулейманов Сулейман Файзуллаевич – кандидат медицинских наук,
старший научный сотрудник, заведующий кафедрой,
кафедра микробиологии, вирусологии, иммунологии и фтизиатрии,*

Бухарский государственный медицинский институт, г. Бухара, Республика Узбекистан

Аннотация: состояние иммунореактивности проанализировано у 52 больных хронической язвенной болезнью двенадцатиперстной кишки (ЯБДК) и у 36 здоровых лиц. У больных выявлена супрессия Т-системы и его субпопуляций, напряжение гуморального звена иммунитета. Традиционные методы лечения не приводили к устранению иммунного дефицита у больных ЯБДК.

Тимоптин в общей дозе 1,0 мг – 1,2 мг (на курс), примененный у больных 2-й группы (n=24), устранял иммунные расстройства, повышал весь спектр клеточного иммунитета, обладал иммунокорректирующим и эрадикационным действием.

Ключевые слова: иммунный статус, язвенная болезнь двенадцатиперстной кишки, Т-система иммунитета, гуморальный иммунитет, иммунотерапия.

Этиопатогенез язвенной болезни двенадцатиперстной кишки (ЯБДК), ассоциированной с *Helicobacter pylori* (НР-инфекцией), связывают с контаминацией слизистой оболочки (СО) гастродуоденальной зоны - ГДЗ (СО желудка - СОЖ и ДК) цитотоксическими штаммами этих бактерий. Показано, что развитие различных форм гастродуоденальной патологии зависит от резистентности макроорганизма, причем патогенные штаммы НР могут проявлять свой цитотоксический эффект только в том

случае, когда снижены иммунобиологические свойства организма человека - на фоне развившихся иммунодефицитных состояний[1-3].

Цель: изучение параметров иммунитета у больных ЯБДК и проведение у них эрадикационной антигеликобактерной и иммунокорригирующей терапии.

Материалы и методы исследований

Обследовано 52 больных ЯБДК, из них 37 (71,2%) мужчин и 15 (28,8%) женщин в возрасте от 23 до 54 лет. Продолжительность язвенного анамнеза составляла в среднем $6,2 \pm 2,4$ года. Диагноз обострения ЯБДК подтверждался эндоскопически. Средний размер (диаметр) язв составлял 0,9 см. Контаминацию СОЖ определяли уреазным тестом. У всех больных выявили высокую степень НР-инфицирования. В зависимости от проведенного лечения больные были распределены на 2 группы: 1-я (n=28) получала схему эрадикации, состоящую из омепразола (40 мг/сут), де nol (480 мг/сут), тинидазол (1000 мг/сут) в теч. 2 нед.; во 2-й (n=24) использовали аналогичную с 1-й группой схему терапии, дополненную тимоптином (Узбекистан) (по 1 мл 0,01% раствора подкожно, через день; на курс 10-12 вливаний).

Клеточный иммунитет изучали с помощью моноклональных антител к CD-рецепторам («SorbentLtd», Россия) Института иммунологии МЗ и СР РФ. Определяли Т-лимфоциты (общая популяция - CD3); Т-хелперы (субпопуляция Тх – CD4); Т-супрессоры (субпопуляция Тс – CD8); В-лимфоциты (субпопуляция CD19) и иммунорегуляторный индекс (ИРИ) - CD4/CD8. Уровень сывороточных иммуноглобулинов классов А, М и G определяли по Mancini (1968).

Иммунологическое обследование проведено на 2-5 сутки с момента госпитализации больного, а также спустя 1 месяц после проведения лечения. Контрольную группу для сравнения иммунологических показателей составили 36 практически здоровых лиц (25-55 лет).

Результаты и обсуждение

При ретроспективном анализе результатов иммунологического обследования, представленных на рис. 1, 2, установлено, что острая фаза ЯБДК сопровождалась снижением уровня общей популяции Т-лимфоцитов (CD3). Выявлены различия в группах с разным исходом эрадикационной терапии: у больных 1-й группы отмечено более низкое содержание Т-клеток в крови, чем у больных 2-й группы. Также в обеих группах отмечался дисбаланс субпопуляций Т-клеток с уменьшением их хелперной доли (CD4) и возрастанием количества супрессоров (CD8); зарегистрировано достоверное снижение ИРИ и В-лимфоцитов (CD19), что указывает на глубокие изменения реактивности у больных ЯБДК.

При обострении ЯБДК в обеих группах наблюдалось достоверное понижение уровней IgA и IgM при одновременном повышении показателей IgG ($p < 0,01$ в 1-й; $p < 0,001$ во 2-й группе), что свидетельствует о нарушениях и в гуморальном компоненте иммунитета.

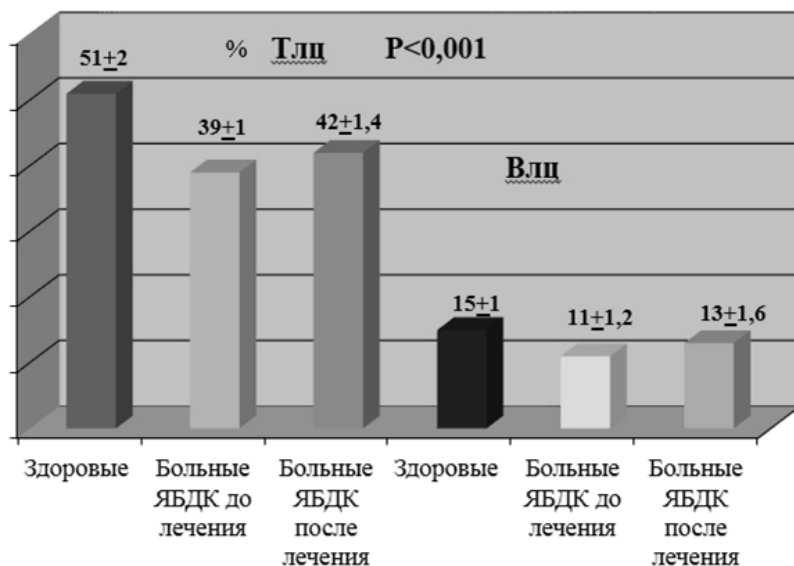


Рис. 1. Показатели клеточного иммунитета у больных 1-й группы в динамике лечения ($M \pm m$)

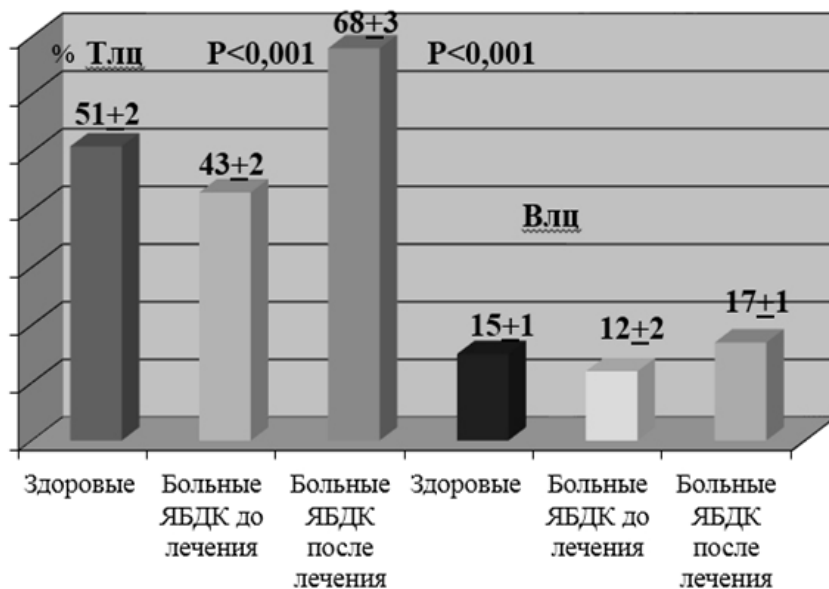


Рис. 2. Показатели клеточного иммунитета у больных 2-й группы в динамике иммунокорригирующего лечения ($M \pm m$)

Формирование пептического дефекта является не только результатом локальных повреждений СО ДК на фоне дисбаланса агрессии и защиты микробной контаминации НР, но и следствием срыва адаптации, дисбаланса в системе иммунитета. ЯБДК у большинства пациентов ассоциирована с кишечным дисбиозом, микробные антигены которой способны вызвать сенсibilизацию и усугублять иммунную недостаточность у больных ЯБДК [1].

Заживление пептического дефекта достигнуто в более короткие сроки при успешной эрадикации НР (в 1-группе – за $24,8 \pm 1,2$ дня с эффективностью эрадикации 59%; во 2-й группе – за $17,3 \pm 0,46$ дня с эффективностью эрадикации 86%).

После лечения у больных 1-й группы сохранялась лимфопения; уровень общей популяции Т-лимфоцитов CD3 (рис. 1) был сниженным, как и её хелперной фракции CD4 ($p<0,01$) при высоком уровне супрессоров CD8, что достоверно отличалось от соответствующих параметров 2-й группы. Снижение ИРИ до 1,5 при норме 2,1 подтверждает разбалансировку в системе CD4/CD8 у пациентов с неэффективной эрадикацией.

У пациентов 2-й группы после проведенной иммунокорректирующей терапии происходило эффективное возрастание количества Т CD3, В-клеток (CD19) (рис. 2) с одновременным увеличением доли Тх (CD4) и ИРИ до 2,3 (норма 2,1), что было намного выше аналогичных значений с 1-й группы ($p<0,001$).

По-видимому, позитивный сдвиг в функционировании Т-клеточного (возрастание CD3, CD4 и снижение CD8) компонента системы иммунитета вносит определенный вклад в эрадикацию НР. Кроме этого, в данной группе наблюдалось возрастание В-лимфоцитов (CD19) и уровня IgA по сравнению с данными до лечения ($p<0,001$).

Таким образом, ЯБДК в стадии рецидива характеризуется глубоким дефицитом большинства параметров иммунной системы организма. Предикторами неэффективной эрадикации являются значительное снижение числа CD3, CD4 и ИРИ, а также уменьшение концентрации IgA. Напротив, клинико-эндоскопическая ремиссия больных 2-й группы характеризуется значительным возрастанием параметров клеточно-гуморального иммунитета, что положительным образом отразилось на результатах эрадикационной и иммунокорректирующей терапии.

Список литературы / References

1. Козлова И.В., Елисеев Ю.Ю., Пахомова А.Л. и др. Прогностические факторы эффективности эрадикационной терапии язвенной болезни двенадцатиперстной кишки // Клин. мед., 2005. № 7. С. 52-55.
2. Циммерман Я.С., Зинатуллин М.Р. Концепция взаимоотношений организма человека и *Helicobacter pylori* // Клин. мед., 1999. № 2. С. 52-56.
3. Reyrai J.-M., Policuc V., Papini E et al. Towards deciphering the *Helicobacter pylori* cytotoxin. // Mol. Microbiol., 1999. № 2 (34). P. 197-204.

Список литературы на английском языке / References in English

1. Kozlova I.V., Eliseev Yu.Yu., Pakhomova A.L. et al. Prognosticheskie faktori effektivnosti eradikatsionnoj terapii jazvennoj bolezni dvenadtsatiperstnoj kishki [Prognostic factors of the effectiveness of eradication therapy of peptic ulcer of duodenum] // Klinicheskaja meditsina [Clinical medicine], 2005. № 7. P. 52-55 [in Russian].
2. Zimmerman Ya.S., Zinatullin M.R. Kontseptsija vzaimootnoshenij organizma cheloveka i *Helicobacter pylori* [The concept of the relationship between the human body and *Helicobacter pylori*] // Klinicheskaja meditsina [Clinical medicine], 1999. № 2. P. 52-56 [in Russian].
3. Reyrai J.-M., Policuc V., Papini E et al. Towards deciphering the *Helicobacter pylori* cytotoxin. // Mol. Microbiol., 1999. № 2 (34). P. 197-204.

INTELLECT OR EMOTIONAL INTELLIGENCE: WHICH COEFFICIENT DETERMINES SUCCESS IN OUR LIFE?

Tabakova V.P.¹, Kurdyuk T.A.² (Russian Federation)

Email: Tabakova432@scientifictext.ru

¹Tabakova Veronika Pavlovna – Student;

²Kurdyuk Tatiana Alexeevna – Student,
FUCULTY CIVIL AND INDUSTRIAL ENGINEERING,
SAMARA STATE TECHNICAL UNIVERSITY,
SAMARA

Abstract: in this article authors review coefficients IQ and EQ for the determination of one of them, which is the basis of success and happiness in our life. Many psychologists explore success and what plays a key role in its coming into being, we will consider the interaction of emotional perception of a person with the outside world and the power of the human brain. So, in this article analyzed parameters of each coefficient, areas of their greatest application and the possibility of their improvement. Thanks to survey we drawn conclusion that also are described in this article.

Keywords: intellect, emotions, success, knowledge, skills, decision making, intelligence development, analysis, self-awareness.

ЭМОЦИОНАЛЬНЫЙ И ИНТЕЛЛЕКТУАЛЬНЫЙ КОЭФФИЦИЕНТЫ: КАКОЙ КОЭФФИЦИЕНТ ОПРЕДЕЛЯЕТ УСПЕХ В НАШЕЙ ЖИЗНИ?

Табакова В.П.¹, Курдюк Т.А.² (Российская Федерация)

¹Табакова Вероника Павловна – студент;

²Курдюк Татьяна Алексеевна – студент,
факультет промышленного и гражданского строительства,
Самарский государственный технический университет,
г. Самара

Аннотация: статья посвящена рассмотрению коэффициентов IQ и EQ для определения одного из них, который положен в основу успеха и счастья в нашей жизни. Так как многие психологи задумывались о том, что же играет ключевую роль в становлении успеха, мы рассмотрим взаимодействие эмоционального восприятия человека с окружающим миром и мощность человеческого мозга. Также в статье анализируются параметры каждого коэффициента, области их наибольшего применения и возможности их совершенствования и, после проведения опроса, приводятся соответствующие результаты.

Ключевые слова: интеллект, эмоции, успех, знания, умения, принятие решений, развитие интеллекта, анализ, самоосознание.

IQ or intelligence quotient demonstrates brainwork and esprit. The people with a high level of IQ can quickly use the information and logical rules. EQ or emotional Intelligence is the ability to control not only your own emotions, but also the emotions of people around you. Such individuals can easily make deals and negotiate. [3]

IQ tests have been very popular for many years. It is worth pointing out that such tests determine brainpower, but not the level of knowledge or erudition. The major criteria of IQ turn out to be mental flexibility, attention and memory.

During our research, we conducted a small survey to find out if success in life is determined by IQ components or EQ components. We asked 84 people to choose the most important qualities for achieving success. Then we analyzed if these components belonged to IQ or EQ. The majority of respondents have chosen a set of different components, in other words, they unconsciously wanted to reach the equilibrium of both coefficients. (Set of components: income level, discipline, objectivity, motivation, luck, composure, communicability, stress resistance, rationality, intellectual flexibility).

Another big difference between IQ and emotional abilities is that IQ is inborn. It reaches a maximum at 17, it remains constant throughout adulthood and declines at old age [2]. However, EQ can be developed. Some examples of methods: Learn to recognize and pay attention to all your emotions, incorporate emotions in your decision-making process, stay present without planning the future or analyzing the past, be aware of nonverbal messages (body language, distance, tone of voice and touch) you send others, use humor and play to relieve stress [5].

IQ is not just knowledge, but some special inborn abilities, so it can't be so easily improved. Social skills are part of EQ and can be developed with some other important constituents, such as self-awareness, self-regulation, motivation and empathy [1]. Indeed, the elements of Emotional intelligence make our lives more fulfilling and happy.

However, it doesn't mean that EQ can completely substitute IQ, because they complement each other.

Also, the impact of EQ and IQ is different in different spheres of life: IQ has a bigger influence at work and in research, but EQ has a bigger influence in a human's personal life and family life [4].

The results of research: the majority of respondents 77% think that the components of EQ are more important for achieving success, 11% of people choose IQ and 12% vote for the balance of both coefficients. Harmony of both quotients is a necessary key to success. And it is only harmony that provides our happiness in life.

References in English / Список литературы на английском языке

1. *Kotova O.U.* EQ against IQ – Which win? // Vestnik of Tomsk State University, 2011 [in Russian].
2. *Stein Steven J., Book Howard E.* Emotional Intelligence and Your Success. Canada: Jossey-Bass Leadership Series, 2011. 351 p.
3. *Goleman D.* Emotional Intelligence: Why It Can Matter More Than IQ. UK: Random House, 2007. 210 p.
4. *Kendra Cherry.* IQ or EQ: Which One Is More Important? [Electronic resource]. URL: www.verywell.com/iq-or-eq-which-one-is-more-important-2795287 Dec. 2016/ (date of access: 10.02.2017).
5. *Segal Jeanne.* Improving Emotional Intelligence // HELPGUIDE.ORG. [Electronic resource]. URL: www.helpguide.org/articles/emotional-health/emotional-intelligence-eq.htm Jun. 2016/ (date of access: 04.02.2017).

References / Список литературы

1. *Котова О.Ю.* EQ против IQ: Кто выиграет? Вестник Томского государственного университета, 2011.
2. *Стайн Стивен, Бук Говард.* Преимущества EQ // Эмоциональная культура и ваш успех, Канада: Canada: Jossey-Bass Leadership Series, 2011. 351 с.
3. *Гоулман Д.* Эмоциональный интеллект // Почему он может намного больше, чем IQ, Великобритания, 2007. 210 с.

4. *Кендра Черри*. IQ или EQ: какой из них более важен? [Электронный ресурс]. Режим доступа: www.verywell.com/iq-or-eq-which-one-is-more-important-2795287. Декабрь, 2016./ (дата обращения: 10.02.2017).
5. *Сегал Жанна*. Улучшение эмоционального интеллекта. [Электронный ресурс]. Режим доступа: www.helpguide.org/articles/emotional-health/emotional-intelligence-eq.htm. Июнь, 2016/ (дата обращения: 04.02.2017).

НАУЧНОЕ ИЗДАНИЕ

ИЗДАТЕЛЬСТВО
«ПРОБЛЕМЫ НАУКИ»

АДРЕС РЕДАКЦИИ:
153008, РФ, Г. ИВАНОВО, УЛ. ЛЕЖНЕВСКАЯ, Д. 55, 4 ЭТАЖ
ТЕЛ.: +7 (910) 690-15-09.

[HTTPS://SCIENTIFIC-PUBLICATION.COM](https://scientific-publication.com)
E-MAIL: [INFO@P8N.RU](mailto:info@p8n.ru)

ТИПОГРАФИЯ:
ООО «ПРЕССТО».
153025, Г. ИВАНОВО, УЛ. ДЗЕРЖИНСКОГО, Д. 39, СТРОЕНИЕ 8

ИЗДАТЕЛЬ:
ООО «ОЛИМП»
УЧРЕДИТЕЛЬ: ВАЛЫЦЕВ СЕРГЕЙ ВИТАЛЬЕВИЧ
117321, Г. МОСКВА, УЛ. ПРОФСОЮЗНАЯ, Д. 140



НАУЧНО-МЕТОДИЧЕСКИЙ ЖУРНАЛ
ИЗДАТЕЛЬСТВО «ПРОБЛЕМЫ НАУКИ»
[HTTP://WWW.SCIENCEPROBLEMS.RU](http://www.scienceproblems.ru)

 **РОСКОМНАДЗОР**
СВИДЕТЕЛЬСТВО ПИ № ФС 77-60218

 НАУЧНАЯ ЭЛЕКТРОННАЯ
БИБЛИОТЕКА
LIBRARY.RU

 **Google**™
scholar

