6. Artjushenko V.M., Korchagin V.A. Ocenka vlijanija pomeh ot radiojelektronnyh sistem na besprovodnye ustrojstva malogo radiusa dejstvija s blokovym kodirovaniem [Estimation of influence of electromagnetic interference from radioelectronic equipment on the function of short-range wireless devices with block coding]. *Jelektrotehnicheskie i informacionnye kompleksy i sistemy*, 2010, vol. 6, no. 4, pp. 10-17.

7. Artjushenko V.M., Abbasova T.S. *Besprovodnye sistemy svjazi* (Wireless Communication System). Moscow, RGUT i S Publ., 2008, 182 p.

8. Artjushenko V.M., Abbasova T.S. *Servis informacionnyh sistem v jelektrotehnicheskih kompleksah* (Service information systems in electrotechnical complexes). Moscow, RGUT i S Publ., 2009, 100 p.

9. Abbasova T.S., Artjushenko V.M. Metody installjacii i proektirovanija jelektricheskih kabel'nyh linij v 10-gigabitnyh sistemah svjazi [Methods of installation and design of electrical cable lines in the 10-gigabit communication systems]. *Jelektrotehnicheskie i informacionnye kompleksy i sistemy*, 2009, vol. 5, no. 2, pp. 10-18.

10. Abbasova T.S., Umudumov O.F. Vybor struktury kompleksa tehnicheskih sredstv dlja servisnogo obsluzhivanija vysokoskorostnyh jelektricheskih traktov strukturirovannyh kabel'nyh sistem [Selection of the technical means structure for maintenance of high-speed electrical paths of structured cable systems]. *Jelektrotehnicheskie i informacionnye kompleksy i sistemy*, 2007, vol 3, no. 4, pp. 21-27.

11. Umudumov O.F., Abbasova T.S. Tehnicheskie sredstva dlja servisnogo obsluzhivanija vysokoskorostnyh jelektricheskih traktov SKS [Technical means for maintenance of of high-speed electrical paths of structured cabling systems]. *Vestnik MGUS*, 2008, no. 1 (4), pp. 77-85.

12. Artjushenko V.M., Abbasova T.S. Obespechenie jelektromagnitnoj sovmestimosti informacionnyh strukturirovannyh kabel'nyh setej [Electromagnetic compatibility of structured cabling information network]. *Privolzhskij nauchnyj vestnik*, 2014, no. 4 (32), pp. 16-22.

13. Artjushenko V.M., Volovach V.I. Jeksperimental'noe issledovanie parametrov spektra doplerovskogo signala, otrazhennogo ot protjazhennogo ob'ekta [Experimental research of parameters of Doppler signal spectrum refl ected from the extended object]. *Prikaspijskij zhurnal: upravlenie i vysokie tehnologii*, 2012, no. 3 (19), pp. 17-24.

14. Artjushenko V.M., Kucherov B.A. Povyshenie operativnosti beskonfliktnogo upravlenija gruppirovkoj kosmicheskih apparatov v uslovijah resursnyh ogranichenij [Improving the effi ciency of confl ict-free group spacecraft under resource limitations] *Jelektrotehnicheskie i informacionnye kompleksy i sistemy*, 2013, vol. 9, no. 3, pp. 59-66.

*Received 13.10.2014*

# УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 004.056

## ИЗУЧЕНИЕ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ В ПОВОЛЖСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ И ШУМЕНСКОМ УНИВЕРСИТЕТЕ ИМ. ЕПИСКОПА КОНСТАНТИНА ПРЕСЛАВСКОГО

*Алексеев А.П.[1], Станев С.С.[2]*

*[1]Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ*

*[2] Шуменский университет им. Епископа Константина Преславского, Шумен, Болгария*

*E-mail: apa2008@rambler.ru*

Рассматриваются вопросы изучения методов защиты информации в двух университетах: ПГУТИ (Россия) и Шуменском университете им. Епископа Константина Преславского (Болгария).

***Ключевые слова:*** криптография, стеганография, стеганология.

### Введение. Постановка задачи

Совершенствование учебного процесса при изучении методов надежной защиты информации является актуальной проблемой. При этом важно не только совершенствовать собственный учебный процесс, но и перенимать опыт вузов,

работающих в этом же направлении, знакомиться с новыми идеями защиты информации.

## Изучение криптографии и стеганографии в ПГУТИ

В Поволжском государственном университете телекоммуникаций и информатики (ПГУТИ) обучают специалистов, работающих в области защиты информации («Информационная безопасность телекоммуникационных систем», специальность – 10.05.02 и «Информационная безопасность», специальность – 10.03.01). В статье рассмотрены вопросы изучения криптографии и стеганографии в рамках дисциплины «Информатика», которая преподается студентам на первом курсе. Дисциплина «Информатика» для указанных специальностей изучается в ПГУТИ в двух семестрах первого года обучения. На лекции отводится 44 часа, на лабораторные работы – 120 часов, на практику – 28 часов, во втором семестре выполняется курсовая работа. Оба семестра завершаются экзаменами.

В рамках дисциплины «Информатика» студенты изучают основные понятия информатики, арифметические и логические основы работы ЭВМ, кодирование информации (сжатие информации, помехоустойчивое кодирование, QR-коды), устройство и принцип действия ЭВМ, системное и прикладное программное обеспечение, сетевые информационные технологии, моделирование телекоммуникационных устройств, а также получают первое представление о методах защиты информации.

Перечислим лабораторные работы, посвященные защите информации:

- «Моделирование аддитивной криптосистемы с помощью программы Multisim (метод гаммирования)»;
- «Моделирование криптосистемы, базирующейся на управляемых операциях (Multisim)»;
- «Скрытая передача информации в графике»;
- «Стеганографические программы Courier и S-Tools»;
- «Сокрытие информации в графике и тексте с помощью математической системы Mathcad»;
- «Моделирование криптосистемы RSA с помощью Mathcad»;
- «Сокрытие информации на HTML-страницах;
- «Скрытая передача данных в субтитрах фильма»;
- «Скрытая передача информации в пакетах, сформированных по протоколу TCP/IP»;
- «Стеганографическая передача данных в звуковых файлах формата WAV и MP3»;
- «Скрытая передача информации методом временного распыления».

В лабораторной работе «Моделирование криптосистемы» студенты с помощью программы Multisim исследуют криптосистему, состоящую из двух арифметико-логических устройств (передающего и приемного). Результаты моделирования сопоставляются с ручными расчётами. Студенты оценивают влияние гаммы на степень криптостойкости системы.

Лабораторная работа «Моделирование криптосистемы, базирующейся на управляемых операциях» является развитием первой работы. В этой криптосистеме помимо операции «Исключающее ИЛИ» для шифрования используется логическая операция «Равнозначность», а также арифметические операции сложения и вычитания [1]. Эти операции при шифровании чередуются в псевдослучайном порядке.

Лабораторная работа «Скрытая передача информации в графике» дает студентам первое представление о стеганографии. Студенты извлекают информацию из рисунков, на которых информация в двоичном виде скрыта в различных местах изображения (рамка рисунка, цвет лампочек на новогодней елке, псевдослучайно расположенные точки).

Следующая лабораторная работа дает первое представление о профессиональной стеганографической программе S-Tools и стеганоанализе. Программа S-Tools перед сокрытием информации выполняет ее шифрование. При извлечении информации, скрытой с помощью программы Courier, студенты анализируют дамп памяти рисунка и, выделяя последние биты, получают скрытое сообщение. В качестве вспомогательного инструмента используется редактор памяти. Моделирование криптосистемы RSA дает студентам возможность детально исследовать шифр с открытым ключом, понять идею цифровой подписи. Выполняемые лабораторные работы показывают обучаемым принципы скрытой передачи информации с помощью различных контейнеров (HTML-страниц, субтитров в фильмах, звуковых файлов).

Лабораторная работа «Скрытая передача информации по протоколу TCP/IP» основывается на преднамеренном изменении длины передаваемых пакетов [2]. Идея лабораторной работы «Скрытая передача информации методом временного распыления» заключается в кратковременной замене рисунка, размещенном на Web-странице, другим

рисунком, содержащим вложение [3]. Рисунок, содержащий скрытно передаваемую информацию, лишь на короткое время появляется на сайте. Все остальное время демонстрируется рисунок, не содержащий сообщения.

Целью этих лабораторных работ является стремление показать студентам принципиальную возможность скрытой передачи информации практически в любом электронном контейнере, а также продемонстрировать возможность увеличения криптостойкости за счет использования нескольких уровней защиты.

Кроме лабораторных работ, вопросы защиты информации изучаются студентами на практических занятиях. Студенты выполняют дешифрацию криптограмм, составленных с помощью классических шифров (Цезаря, Атбаша, квадрата Полибия, таблицы Виженера, метода перестановок, шифра Плейфейра, аффинных преобразований, метода гаммирования). На практических занятиях рассматривается структура мультимедийных файлов, что облегчает понимание идей стеганографических методов защиты информации.

При выполнении курсовых работ студенты извлекают скрытую информацию из HTML-контейнеров. При этом передаваемая информация распылена по нескольким контейнерам, а перед распылением сообщение, преобразованное в двоичный код, шифруется путем выполнения перестановок битов с помощью матриц.

Проблемам защиты информации посвящено достаточно большое число дипломных работ. Приведем примеры их тематики:

- «Разработка шифра с большим числом математических преобразований»;
- «Разработка и исследование методов обнаружение вложений в графических контейнерах путем проверки статистических гипотез»;
- «Адаптивный шифр со скрытым ключом»;
- «Разработка атаки на шифр «Графические матрицы» с помощью нейронных сетей».

За последние пять лет в ПГУТИ защищено три диссертации на соискание ученой степени кандидата технических наук, тематика которых связана с криптографией и стеганографией [4-6].

## Преподавание криптографии и стеганографии в ШУ

В Шуменском университете (ШУ) вопросы криптографии и стеганографии преподаются с 2004 г. в рамках ряда учебных дисциплин для студентов специальностей «Управление системами безопасности» и «Информатика» (специализация «Компьютерная информатика» и «Компьютерные информационные технологии»). С 2010 г. на Факультете математики и информатики введена учебная дисциплина «Компьютерная стеганография» (пока единственная в вузах Болгарии).

Учебные занятия с ярко выраженным исследовательским характером «плавно переходят» в дипломные работы, а также диссертации в области компьютерной и сетевой стеганографии. Следуя за быстрым развитием научных исследований, каждый год изменяется содержание учебных дисциплин. Последнее изменение было введение в учебные программы сетевой стеганографии. Студенты имеют возможность реализовать свои идеи по разработке новых шифров, критериев для сравнения различных стеганографических методов передачи информации, программ для шифрования, выбора шифров в целях дополнительного повышения криптостойкости стеганографической передачи и многое другое. Благодаря работе преподавателей и студентов были определены основные термины компьютерной и сетевой стеганографии на болгарском языке, близкие по смыслу к терминам на английском и русском языках [7]. Например, было предложено ввести как стандартный в Болгарии термин «стеганология» как совокупность стеганографии и стеганоанализа применительно к их компьютерной реализации, а также «стегоключ» вместо русского «стеганографический ключ». Исследовалась эффективность созданных студентами стеганографических программ по сравнению с популярными доступными в Internet программами [8].

Для студентов было разработано методическое руководство по практической компьютерной стеганографии, в котором рассмотрены вопросы симметричного и асимметричного шифрования, применение стеганографических программ для создания стегофайлов и использование методов сетевой стеганографии для передачи стеганографических ключей.

При изучении теоретических вопросов стеганологии студенты пользуются монографией «Стеганологическая защита информации» [9]. Перечислим ее основные разделы:

- «Введение в стеганологию»;
- «Методы и средства компьютерной стеганографической защиты информации»;
- «Методы и средства сетевой стеганографической защиты информации»;
- «Стегоанализ и проблемы защиты информации»;
- «Стеганология в параллельных компьютерных средах»;

- «Стеганологические подсистемы защиты информации».

Впервые в болгарских научных работах был сформулирован термин «стегоинцидент» и предложены организационные и программно-аппаратные способы его предотвращения. Предлагаемая в монографии модель подсистемы программной стеганологической защиты информации как элемент комплексной системы защиты информации состоит из двух модулей. Стеганографический модуль выбирает подходящий мультимедийный контейнер для сокрытия информации и передачи стегоключей способом сетевой стеганографии. Он связан с подсистемой криптографической защиты. Модуль стегоанализа на базе параллельных программ предотвращает утечки из организации информации, скрытой стеганографическими методами. Исследования и практические занятия по стеганологии проводятся в научно-исследовательской лаборатории «Компьютерная безопасность», в которой постоянно работает творческая студенческая группа и три аспиранта. В 2012 г. в лаборатории была установлена разработанная сотрудниками университета компьютерная кластерная система «Радиан-М» с общей производительностью 180 GFLOPS и энергетической эффективностью 19 MFlops/watt.

В ШУ защищены две диссертации на соискание докторской степени в области информатики. В работе [10] был предложен эффективный параллельный стеганографический алгоритм на базе метода LSB с использованием восьмеричной системы счисления. Разработан формат для структуры полей стегоключа. Предложена практическая процедура передачи стегофайлов с использованием мультимедийных контейнеров для основных секретных сообщений. Передача 1024 байтовых стегоключей осуществляется сетевым протоколом RDP методом временного кодирования секретных символов ключа между символами открытых сообщений. Исследована помехозащищённость секретного стегоканала и сформулированы направления ее улучшения. Проведено сравнение этого подхода передачи стегоключа и варианта с применением разработанного в [2] метода сетевой стеганографии по протоколу TCP.

В [11] разработаны аналитические и статистические модели для оценки воздействия возможных угроз в информационных системах и для оценки потерь в компьютерных сетях. На их базе предложены количественные оценки эффективности стеганографических систем защиты информации. Сформулирован комплексный показатель оценки эффективности процесса стегоанализа. Разработанные программы для кластерной системы позволяют проводить стегоанализ в режиме реального времени, что необходимо при реализации защиты информации организаций. Эксперименты показали, что предложенные алгоритмы позволяют обнаружить сокрытую информацию с коэффициентом встраивания сообщения ниже нижней границы, указанной в научных публикациях для аналогичных алгоритмов.

В обеих диссертациях были разработаны параллельные программы стеганографии и стегоанализа и показаны их преимущества по сравнению с последовательными программами [12]. Достигнута эффективность обнаружения сокрытых сообщений свыше 87% при $(n-1)$-кратном сокращении времени выполнения последовательных программ при параллельно работающих $n$ процессоров (ядер).

Лаборатория «Компьютерная безопасность» участвует в междисциплинарных проектах. В результате сотрудничества с другими организациями были опубликованы совместные статьи [13-14], подготовлена диссертация [15], в которой создана модель стегозащиты конфиденциальной информации болгарского заграничного военного контингента. Студентами было защищено свыше 15 дипломных работ в области стеганографии. При участии преподавателей и студентов было реализовано 5 проектов по стеганологии, финансированных Фондом научных исследований ШУ. Кроме разработанных стегопрограмм и научных публикаций, важным результатом является то, что постепенно формируется новое научное направление (не только для ШУ) – компьютерная стеганография и стегоанализ в параллельных вычислительных средах.

## Выводы

По результатам исследований, проведенных преподавателями совместно со студентами в двух вузах России и Болгарии, было опубликовано несколько монографий и учебников [9; 16-18], сделано свыше 70 докладов на научно-технических конференциях, получены патенты и опубликованы статьи в научно-технических журналах, защищены магистерская диссертация, три диссертации на соискание степени кандидата технических наук и две докторские диссертации. Между ПГУТИ и ШУ заключен Договор о творческом сотрудничестве.

## Литература

1. Алексеев А.П., Жеренов Ю.В., Орлов В.В. Моделирование криптосистемы с управляемыми операциями с помощью MULTISIM // ИКТ. Т. 7, № 4, 2009. – С. 78-82.
2. Орлов В.В., Алексеев А.П. Способ стеганографической передачи информации в сети TCP/IP. Патент RU 2463670.

3. Алексеев А.П., Макаров М.И. Адаптивный шифр с пространственно-временным распылением информации // ИКТ. Т. 9, №1, 2011. – С. 62-66.
4. Аленин А.А. Разработка и исследование методов скрытой передачи информации в аудиофайлах. Автореф. дисс. к.т.н. Самара, 2012.
5. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях. Автореф. дисс. к.т.н. Самара, 2012.
6. Макаров М.И. Разработка и исследование методов скрытой распределенной передачи сеансовых данных в телекоммуникационных сетях. Автореф. дисс. к.т.н. Самара, 2013.
7. Станев. С., Галяев В. Семантична еквивалентност на основните термини на компютърната стеганология в българските, английските и руските научни публикации. // Сборник научни трудове Международна научна конференция MATTEX2012. Шумен, 2012. – С. 119-126.
8. Станев С., Железов С., Великова Т., Неделчева В. За ефективността на стеганографските програми. / /Сборник научни трудове. Научна конференция с межд. участие «40 години Шуменски университет». Том ФМИ, Шумен, 2011. – С. 97-102.
9. Станев С. Стеганологична защита на информацията. Университетско издателство «Епископ Константин Преславски». Шумен, 2013. – 120 с.
10. Параскевов Х. Методи за стеганографска защита на информация в компютърни мрежи. Автореф. на дисер. за получ. на научно-образователна степен «доктор». Шумен, ШУ «Еп. К.Преславски», 2014.
11. Железов С. Оценка на ефективността на системи за защита на информацията в компютърните системи. Автореф. на дисер. за получ. на научно-образователна степен «доктор». Шумен, ШУ «Еп. К.Преславски», 2014.
12. Станев С., Железов С., Якимов И. Реализация на паралелен стеганализ с клъстерна система // Сборник научни трудове Международна научна конференция «Съвременни методи и технологии в научните изследвания». Варна, 2012. – С. 122-127.
13. Stanev S., Hristov H., Dimanova D. Aproaches for Stego Defense of Sensitive Information from Inside Leakage // Journal Science Education Innovation. Vol.1, 2013. – P. 126 -132.
14. Nachev A., Zhelezov S. Assessing the efficiency of information protection systems in the computer systems and networks // Information Technology and Security. № 1(3), Special issue, Kiev, 2013. – P. 79-85.
15. Кръстев К. Повишаване на сигурността на участниците в мисии зад граница. Дисер. за получ. на научно-образователна степен «доктор». София, УНИБИТ, 2014.
16. Алексеев А.П. Информатика 2001. М.: Солон-Р, 2001. – 364 с.
17. Алексеев А.П. Информатика 2007. М.: Солон-Пресс, 2007. – 608 с.
18. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации: учебное пособие. Самара: Изд-во ПГУТИ, 2010. – 330 с.

*Получено 19.12.2014*

Алексеев Александр Петрович, к.т.н., профессор Кафедры информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 228-00-57 E-mail: apa2008@rambler.ru

Станев Станимир Стоянов, д.т.н., профессор, заведующий Кафедрой компьютерных систем и технологий Шуменского университета им. Епископа Константина Преславского (Болгария). Тел. 003-598-999-079-14. E-mail: stan_staven@yahoo.com

## CRYPTOGRAPHY AND STEGANOGRAPHY STUDY IN POVOLZHSKIY STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS (SAMARA, RUSSIA) AND SHUMEN UNIVERSITY (SHUMEN, BULGARIA)

Alekseev A.P., Stanev S.S.

The problems of cryptography and steganography are taught at two universities - PGUTI (Sama-ra) and the University of Shumen (Bulgaria) on basis of scientific cooperation agreement. It is a brief overview of the initial course content of «Informatics» in PSUTI. The course teaches students to learn the basic concepts of computer science and get a first glimpse of data protection methods of cryptography and steganography. There are basic ideas of published works. The first work on steganography in PSUTI were published in 2002. A few original ideas are described. For example, in the cryptosystem manage operations in addition to the exclusive-OR is used

to encrypt the logical equivalence of the operation, as well as arithmetic operations of addition and subtraction. Another cryptosystem uses a secure communication protocol TCP / IP. Thus there is a deliberate change in the length of the transmitted packets. In Shumen University since 2004 cryptography and steganography are studied in several disciplines for students of «Safety Management» and «Computer Science». In 2010, the Faculty of Mathematics and Informatics in Bulgaria introduced the course «Computer Steganography» for the first time. Research on steganology was conducted by the scientific research Laboratory «Computer Security», which was developed by the cluster computer system with a total capacity of 180 GFLOPS and the energy efficiency of 19 MFLOPS / Watt. According to the study conducted by the teachers together with students at two universities, several monographs and textbooks have been published as well as articles in scientific and technical journals, more than 70 scientific papers were presented at scientific conferences, the patents were received, a number of theses have been prepared and defended. An agreement on creative collaboration was concluded between PSUTI and SHU universities.

***Keywords:*** *cryptography, steganography, steganologiya.*

**Alexeev Alexander Petrovich**, PhD in Technical Science, Professor of Department of Information and Computer Engineering, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel. 7 846 228 00 57. E-mail: apa2008@rambler.ru
**Stanev Stanimir Stoyanov**, Doctor of Technical Science, Professor, Head of Department of Computer Systems and Technologies, Shumen University, Bishop Constantine of Preslav, Shumen, Bulgaria. Tel. +3 598 999 079 14 E-mail: stan_staven@yahoo.com

**References**

1. Alekseev A.P., Zherenov Ju.V., Orlov V.V. Modelirovanie kriptosistemy s upravljaemymi operacijami s pomoshh'ju MULTISIM [Modeling criptosystem with operated operations of enciphering by means of the program MULTISIM] *Infokommunikacionnye tehnologii*, 2009, vol. 7, no. 4, pp. 78-82.

2. Orlov V.V., Alekseev A.P. *Sposob steganografi cheskoj peredachi informacii v seti TCP/IP* [Steganographic method of information transmission in the TCP/IP network]. Patent RF no. 2463670, 2012.

3. Alekseev A.P., Makarov M.I. Adaptivnyj shifr s prostranstvenno-vremennym raspyleniem informacii [Adaptive cipher with spatial-time dispersion of the information]. *Infokommunikacionnye tehnologii*, 2011, vol. 9, no. 1, pp. 62-66.

4. Alenin A.A. *Razrabotka i issledovanie metodov skrytoj peredachi informacii v audiofajlah*. Avtoref. diss. kand. techn. nauk. Samara, PSUTI Publ., 2012, 16 p.

5. Orlov V.V. *Metody skrytoj peredachi informacii v telekommunikacionnyh setjah*. Avtoref. diss. kand. techn. nauk. Samara, PSUTI Publ., 2012, 16 p.

6. Makarov M.I. *Razrabotka i issledovanie metodov skrytoj raspredelennoj peredachi seansovyh dannyh v telekommunikacionnyh setjah*. Avtoref. diss. kand. techn. nauk. Samara, PSUTI Publ., 2012, 16 p.

7. Stanev. S., Galjaev V. Semantichna ekvivalentnost na osnovnite termini na kompjutrnata steganologija v blgarskite, anglijskite i ruskite nauchni publikacii. *Trudy Mezhdunarodna nauchna konferencija MAT-TEH2012*. Shumen, 2012, pp. 119-126. (In Bulgarian)

8. Stanev S., Zhelezov S., Velikova T., Nedelcheva V. Za efektivnostta na steganografskite programi. *Sbornik nauchni trudove. Nauchna konferencija s mezhd. uchastie «40 godini Shumenski universitet»*. Tom FMI, Shumen, 2011, pp. 97-102. (In Bulgarian)

9. Stanev S. *Steganologichna zashhita na informacijata*. Universitetsko izdatelstvo «Episkop Konstantin Preslavski». Shumen, 2013. – 120 p. (In Bulgarian)

10. Paraskevov H. *Metodi za steganografska zashhita na informacija v kompjutrni mrezhi*. Avtoref. na diser. za poluch. na nauchno-obrazovatelna stepen «doktor». Shumen, ShU «Ep. K.Preslavski» Publ., 2014. (In Bulgarian)

11. Zhelezov S. *Ocenka na efektivnostta na sistemi za zashhita na informacijata v kompjutrnite sistemi*. Avtoref. na diser. za poluch. na nauchno-obrazovatelna stepen «doktor». Shumen, ShU «Ep. K.Preslavski» Publ., 2014. (In Bulgarian)

12. Stanev S., Zhelezov S., Jakimov I. Realizacija na paralelen steganaliz s klasterna sistema. *Sbornik nauchni trudove Mezhdunarodna nauchna konferencija «Sovremenni metodi i tehnologii v nauchnite izsledvanija»*. Varna, 2012, pp. 122-127. (In Bulgarian)

13. Stanev S., Hristov H., Dimanova D. Aproaches for Stego Defense of Sensitive Information from Inside Leakage. *Journal Science Education Innovation*, 2013, vol. 1, pp. 126-132.

14.Nachev A., Zhelezov S. Assessing the efficiency of information protection systems in the computer systems and networks. *Information Technology and Security*, 2013, vol. 1, no. 3, Special issue, Kiev, pp. 79-85.

15.Kr'stev K. *Povishavane na sigurnostta na uchastnicite v misii zad granica.* Diser. za poluch. na nauchno-obrazovatelna stepen «doktor». Sofija, UNIBIT Publ., 2014. (In Bulgarian)

16.Alekseev A.P. *Informatika 2001* [Informatics 2001]. Moscow, Solon-Press Publ, 2001, 364 p.

17.Alekseev A.P. *Informatika 2007* [Informatics 2007]. Moscow, Solon-Press Publ, 2007, 608 p.

18.Alekseev A.P., Orlov V.V. *Steganografi cheskie i kriptografi cheskie metody zashhity informacii* [Steganographic and cryptographic methods of information security]. Samara, PGUTI Publ., 2010, 330 p.

*Received 19.12.2014*

## ПОЗДРАВЛЯЕМ С ЮБИЛЕЕМ!

### Я.С. Шифрину – 95 лет

23 апреля 2015 года специалисты в области радиотехники и электроники отмечают юбилей патриарха антенной техники, создателя статистической теории антенн (СТА) Якова Соломоновича Шифрина.

Профессор Я.С. Шифрин – ветеран Второй мировой войны, куда он пошел добровольцем Ленинградской Армии Народного ополчения после окончания с отличием физического факультета ЛГУ в 1941 году. Был откомандирован в Военную Краснознаменную академию связи им. С.М. Буденного и после окончания с отличием академии и кратких курсов по радиолокации командовал до конца войны одной из новейших по тому времени систем орудийной наводки в войсках ПВО. Летом и осенью 1943 г. принимал непосредственное участие в боях, награжден орденами и медалями. После войны служил в Военной инженерной радиотехнической академии им. Л.А. Говорова (г. Харьков), пройдя путь от адъюнкта до профессора и начальника кафедры. После увольнения из Советской Армии заведовал кафедрой и работал профессором в Харьковском национальном университете радиоэлектроники.

Крупнейшим достижением Я.С. Шифрина стало создание СТА, получившей всемирное признание в качестве одного из краеугольных камней современной теории и практики применения антенн. Другими его научными вкладами являются разработка теории антенно-фидерных устройств с нелинейными элементами и вопросов диагностики фазированных антенных решеток. Профессору Шифрину принадлежит первое в СССР детальное исследование явления дальнего тропосферного распространения (рассеяния) радиоволн.

За полвека научно-педагогической деятельности Яков Соломонович вырастил более 20 докторов и 50 кандидатов наук, опубликовал сотни научных работ и 12 монографий. В 1983 г. он был награжден премией им. А.С. Попова Академии наук СССР с формулировкой «за работы в области СТА, внесшие фундаментальный вклад в теорию и технику антенн», а тридцать один год спустя – медалью Outstanding Career Award от European Microwave Week – Европейской Микроволновой Ассоциации «за выдающуюся профессиональную деятельность в знак признания лица, карьера которого являет собой пример выдающихся достижений в области СВЧ», что говорит о поистине неподвластной времени творческой активности и многолетней неиссякаемой энергии юбиляра.

В своем кратком выступлении на конференции EMA (Рим, октябрь, 2014) при вручении награды, которая представляет собой бронзовую медаль с изображениями эмблемы ассоциации и имени награжденного, Яков Соломонович поблагодарил Совет директоров, отметив значимость EMA для микроволнового сообщества Европы. «Я рассматриваю свое награждение как признание достижений советской науки в теории и технике СВЧ Европейским научным сообществом. Из-за существовавшего долгие годы «железного занавеса» выдающиеся работы советских ученых в области прикладной электродинамики, да и сами их имена на Западе были малоизвестны. Пользуясь возможностью, я хочу назвать некоторых из уже ушедших замечательных ученых, моих друзей, внесших значительный вклад в микроволновую науку. Это академики А. Пистолькорс, Л. Бахрах, профессора Я. Фельд, Е. Зелкин, А. Вольперт, М. Конторович, В. Шестопалов».

Редколлегия, авторы и читатели нашего журнала присоединяются к поздравлениям и добрым пожеланиям в адрес замечательного человека и выдающегося ученого Якова Соломоновича Шифрина.

*Соб. инф. ИКТ*