ОБУЧЕНИЕТО И ИЗСЛЕДВАНИЯТА ПО СТЕГАНОЛОГИЯ В ШУМЕНСКИЯ УНИВЕРСИТЕТ „ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ” *

СТАНИМИР С. СТАНЕВ

TEACHING AND RESEARCHES IN STEGANOLOGY AT THE UNIVERSITY OF SHUMEN

STANIMIR S. STANEV

ABSTRACT: *The report examines the researches on steganology in University of Shumen and challenges in teaching steganography of students of computer sciences at the same university as a component of their professional training. The outcome of this training are bachelors and masters theses, practical activities of experimentation of stego software and steganology in a parallel computing environment, joint scientific publications of lecturers and students.Short review of the contents of textbooks, lectures and labs is done.*

KEYWORDS: *steganology, steganography.*

Стеганографията е научно-приложна област, изкуство, съвкупност от технически умения и за начините за скриване на факта на предаване (наличие) на информация. Класическата стеганография има хилядолетна история и предлага стотици методи за скриване на съобщения (симпатични мастила, микроточки, тайни канали, холография, и др.). Техни наследници са методите на компютърната и мрежовата стеганография – самостоятелни научни направления на информационната сигурност, изучаващи проблемите на създаване на компоненти със скрита информация в явната информационна среда,

* Разработката е частично финансирана от фонд „Научни изследвания” на Шуменския Университет „Епископ К. Преславски” по проект РД 08-238 /13 март 2014.

генерирана от компютърните системи и мрежи. Днес стеганологията (термин, обобщаващ стеганографията и стеганализа) се развива бурно, и това води неизбежно и до изменения и развитие на използваните термини, понятия, походи и методи. Актуалността на тези проблеми изисква запознаването с основите на съвременната стеганология на по-широк кръг от специалисти, чиято задача е не само разработването, анализа или противодействието на стеганосредствата, но и квалифициран избор на съществуващите стеготехнологии и тяхното умело използване за решаване на конкретни приложни задачи в областта на защитата на информацията. Това е особено важно за бъдещите специалисти в областта на компютърните науки.

Целта на настоящата работа е да обобщи първите резултати от обучението на студентите от специалност „Информатика” в Шуменския Университет по проблемите на компютърната и мрежова стеганография, като компонент на тяхната професионална подготовка по информационна сигурност, и провеждането на изследванията в тази област в Университета.

Предисторията на обучението и изследванията по стеганография започна в началото на второто хилядолетие, когато в учебния план на специалност „Национална сигурност” бе включена учебната дисциплина „Компютърна и мрежова сигурност”. Тогава група преподаватели с добра предварителна подготовка в областта на информационната сигурност започна подготовката по обучение на студентите от специалности ”Информатика”, „Национална сигурност” и „Комуникационни и информационни системи” по приложните аспекти на стеганологията. През 2002 год. Университетското издателство на ШУ отпечата учебно пособие по посочената дисциплина за нуждите на дистанционното обучение на студенти [1]. На базата на анализа на модерните тенденции в развитие на компютърната сигурност, в него бе включен и параграф за стеганографията, нейното използване и перспективи. Последва сериозен анализ на достъпните информационни източници и решението на група преподаватели от катедра „Компютърни системи и технологии” да се започнат теоретични и практически изследвания в това

многообещаващо направление за научно израстване на преподаватели и обучаеми. Бе формирана студентска проблемна група, включваща и преподаватели, работещи по проекти, която започна с анализ на параметрите на достъпните в Интернет стегопрограми и експерименти с тях. От 2004 година започна разработването на студентски дипломни работи по стеганография, с приложни приноси – основно собствени стегопрограми. На студентите се даде възможност да предлагат, анализират и внедряват своите разработки. В съавторство със своите научни ръководители, студентите изнесоха статии в научни конференции, което допълнително ги мотивира. Създаването на компютърната лаборатория „Компютърна сигурност” беше естествен завършек на тази предварителна дейност.

Поради разнообразието и сложността на проблематиката бе предложено успоредно с научните проекти да се започне обучение на по-широк кръг бъдещи специалисти и изследователи. Събран бе достатъчно материал за лекции и упражнения, и бе решено компютърната стеганография да се обособи като самостоятелна дисциплина в учебния план на специалност „Информатика” (бакалаври). Идеята още от самото начало бе това да бъде непрекъснат и спираловиден процес, започващ от обучението в учебна дисциплина с ярко изразен изследователски характер, и преминаващ в работа в студентски проблемни групи, дипломни работи, магистърски програми, специализации и докторантури в областта на компютърната и мрежова стеганография. През 2010 г. ФС на Факултета по математика и информатика на ШУ реши учебната дисциплина „Компютърна стеганография” да се добави като избираема за студентите от четвърти курс в бакалавърска степен. По наша информация до тогава (и сега) такава учебна дисциплина не се изучаваше в българските висши учебни заведения.

Учебната дисциплина има силно изразен учебно-изследователски характер. Чрез задачите за самостоятелна подготовка и указанията на преподавателите студентите са в непрекъснат допир чрез Интернет с актуален софтуер – например се започва с изтегляне и тестване на версия за тестване на

Invisible secrets и се достига до изучаването на характеристиките на най-модерните в момента комерсиални продукти на Wetstone и BlackBone Security. Като курсови работи се задава търсене и изтегляне на freeware и shareware стегопрограми в Интернет, тяхното тестване с цел определяне на ефективността им и др., намиране на актуална информация за различни стеганометоди и нейния превод от английски и руски език, разработване на реферати по определени проблеми на стеганологията. Преподавателите предлагат за анализ и сравнение разработени от преподавателите и дипломантите стегопрограми, използват и някои от своите научни разработки и ги обсъждат на семинарните занятия със студентите. Студентите имат възможност да се запознаят и предлагат свои идеи в уточняване на терминологията, параметрите за изследване, критерии за сравнение на стеганографски и стегоаналитични програми, избор на шифри с цел допълнително осигуряване на стеганографско предаване, идеи за стеганалитични програми и др. За да се засили интереса на студентите към учебния материал, още в началото им се предлагат и исторически примери от нашето минало. Нов момент за тях е нашето класифициране на използваните от българските революционни комитети и от Васил Левски средства на тайнопис със симпатично мастило и шаблоните, наричани „скари” и ”лозинки”, за вмъкване на буквите на таен текст в обикновени писма като стеганографски средства. Тези скари са аналогични на известните по това време в Европа скари на Кардан (Cardan grille). Разглежда се развитието на стеганографията в ново време с примери от използването й и от престъпни организации и от тайните служби, с аферата в САЩ през 2010 год. с участието на руски агенти и др. На студентите бе предложена за обсъждане наша оригинална схема на класификацията на високотехнологичната стеганография. Бе отбелязано, че с развитие на съвременната стеганография ще се развиват и променят класификациите, тъй като сега все още е трудно да се направи такава, която да покрие всички варианти, и общите сечения между тях. На български език се дефинираха основни термини на компютърната и мрежова стеганография и благодарение на

активната работа на студентите по своите курсови задачи се направи сравнение и се намериха най-близките по смисъл еквивалентни термини на английски и руски език [2]. Интересен е друг пример от семинарните занятия. Студентите сами логически достигнаха до термина стеганология – обобщаващ термин за стеганографията и стеганализа, по аналогия с криптологията, състояща се от криптография и криптоанализ. После с изненада открихме, че не толкова отдавна – през 2005 година, такъв термин е приет от световната научната общност. Въведен бе терминът ефективност на стегосистемата като съвокупност от специализиран софтуер и хардуер, а не само като метод за стеганография [3]. За първи път у нас бяха формулирани термините "стегоинцидент" и „стегозащита” [4].

Следвайки бързото развитие на научното направление и постоянното внедряване на нови методи и програми, заедно с натрупвания опит в преподаването всяка година се променяше и учебното съдържание на дисциплината. Последната промяна бе въвеждане на тема по мрежовата стеганография – класифициране на прилаганите методи, тяхното описание и анализ на действието им. Текущият вариант на програмата по учебната дисциплина „Компютърна стеганография” е с хорариум 60 часа аудиторна заетост, от които 30 часа лекции и 30 часа семинарни занятия, провеждани в учебни зали и лаборатория „Компютърна сигурност”. Лекционният материал включва темите „Проблеми на компютърната и мрежовата сигурност” (в нея са включени общи въпроси на компютърната сигурност, заплахи и атаки и походи за защита на компютърните системи и мрежи), „Криптографски алгоритми в стеганографията”, „Основи на компютърната стеганография”, „Избор на стеганографски контейнери”, „Мрежова стеганография”, „Системи за скрита идентификация (Цифрови водни знаци, отпечатъци)”, „Стеганализ и ефективност на стеганографските алгоритми и програми”, „Разработване на системи за защита”.

На семинарните занятия от практическа гледна точка се обсъждат проблеми като „Стандарти за информационна сигурност”, „Политики на сигурност”, „Криптиране на информа-

цията”, „Софтуер за криптиране на съобщения в Интернет”, „Алгоритми и програми за стеганографска защита на текстови файлове”, „Разработване на собствени програми за реализация на метода LSB”, „Използване на аудиоконтейнери и видеопоследователности за скриване на информация”, „Анализ на методи и средства за мрежова стеганография”, „Високотехнологични стеганографски походи за мобилни компютърни устройства”, „Видове стеганализ”, „Програми за стеганализ”, „Сравнителен анализ на стегопрограми”, „Изследване на ефективността на софтуер за стеганализ”.

За усвояване на теоретичните въпроси на стеганологията студентите с успех използват монографията „Стеганологична защита на информацията” (фиг.1), която съдържа следните глави: Увод в стеганологията, Методи и средства за компютърна стеганографска защита на информацията, Методи и средства за мрежова стеганографска защита на информацията, Защита от компютърни стегометоди чрез стеганализ, Стеганология в паралелни компютърни среди и Стеганологични подсистеми за защита на информацията (СПСЗИ) [4].

За студентите е разработено методическо ръководство по практическа стеганография, в което са разработени въпроси по симетрично и асиметрично криптиране, използване на стеганографски програми за създаване на стегофайлове и използване на методите на мрежовата стеганография [5].

Откроиха се и някои учебно-методически проблеми при обучението по компютърна стеганография. Експерименталната методика на провеждането на занятията доведе до ясното разделение на студентите на две основни групи. Първата, съставена от студенти, склонни и способни за творческо усвояване на новите знания, желаещи да участват в изследователска работа. Втората група, състояща се от повече на брой студенти, не желаеше да се откъсва от традиционните методи на преподаване и учене, показа липса на желание и навици за по-самостоятелна работа.В бъдеще трябва да се потърсят други механизми за мотивиране на творческата работа

на всички студенти, избрали за изучаване дисциплината „Компютърна стеганография”.

Първите дипломни работи по проблеми на стеганографията на студенти от магистърски програми по информатика в ШУ бяха успешно защитени през 2004 год., до 2014 год. в тази област са защитени общо 15 дипломни работи само от студенти по Информатика, и 3 дипломни работи на студенти от Факултет АПВОКИС на НВУ, ръководени от проф. Станев, д-р Железов, д-р Параскевов и проф. Начев. Примери за темите на дипломните работи са „Ефективност на програми за стеганографска защита”, „Изследване на възможностите на съвременните програми за стеганоанализ”, „Анализ на възможностите на мрежови протоколи и устройства за мрежова стеганография”, „Изследване на възможностите за стеганографска паралелна обработка с клъстерна компютърна система”. В тези изследвания бяха разработени практически критерии за ефективност на алгоритмите и стегопрограмите, база от данни с хипервръзки за достъпния в мрежата стеганографски и стеганалитичен софтуер.

През 2014 година са защитени две дисертации за получаването на докторска степен по информатика, и е присвоено професорско звание в областта на компютърната сигурност. В са развити аналитични и статистически модели за оценка на въздействието на възможните заплахи за информацията в информационните системи, както и за оценка на загубите в областта на компютърните мрежи. Формулиран е комплексен показател за оценка на ефективността на системи за информационна сигурност. В дисертацията са разработени подходи и алгоритми за паралелен стеганализ с клъстерна система в реално време Получените резултати с успех са докладвани на престижни научни форуми [7, 8].

В [9] е предложен ефективен паралелен стегоалгоритъм алгоритъм, основан на метода LSB с използване на осмична бройна система. Предложен е формат за структурата на полета на стегоключовете. Показана е практически процедура за предаване на стегофайловете с използване мултимедиен контейнер за основните тайни послания и предаване на 1024 битови

стегоключове чрез мрежов протокол RDP с времево кодиране на секретните символи на ключа между символите на явно съобщение.

Фиг. 1

През 2014 г. бе разработена и дисертация за получаване на научно-образователна степен „доктор”, в която има един раздел, свързан със стеганографията [10]. Един от резултатите е разработването на модел за предотвратяване на изтичане на поверителна информация чрез стегоканал в условията на задграничен военен контингент [11].

Изследванията по стеганология се извършват в научно-изследователската лаборатория на ФМИ „Компютърна сигурност”, в която работят преподаватели и докторанти от катедра КСТ на ФМИ, както и проблемна студентска група (от студенти от бакалавърски и магистърски програми по „Информатика”). През 2011 в лабораторията бе монтирана клъстерна компютърна система „Радиан-М”, разработена от колектив от ФМИ и ФТН на ШУ (фиг. 2). Системата има 32 ядра с обща производителност

180 GFLOPS. С нея екипът от изследователи започна работа в ново направление – използване на клъстерна система за паралелна стеганография и стеганализ. В лабораторията са разработени няколко проекта, финансирани от фонда „Научни изследвания” на ШУ – Оценка на възможностите за откриване и предотвратяване на разпространението на скрита чрез стеганографски методи информация (2008), Изследване на софтуер за ОС XP И VISTA – базирани платформи за мрежова защита и откриване на стеганографски съобщения (2009), Изследване на ефективността на алгоритми и софтуер за стеганографска защита на информация в елементи на 3D виртуални обекти (2010), Изследване на възможността за използване на високопроизводителна компютърна система за стеганализ (2011) и др. През 2014 г. се работи по проект за модел на паралелна стеганалитична подсистема за защита на информацията. Лаборатория „Компютърна сигурност” участва и в интердисциплинарни проекти [12, 13, 14].

Част от оригиналните резултати от изследванията в лабораторията ставаха веднага достъпни за обсъждане по време на семинарните упражнения по дисциплината. В проблемната студентска групата по стеганография работеше и ученичката Катерина Велчева от Шуменската математическа гимназия. През периода 2009 – 2011 год. благодарение на отличната си подготовка като програмист и сътрудничеството си с лабораторията, тя успешно разработи и защити проекти по стеганография към Ученическия Университет в Пловдив. Публикува статии по въпроса в няколко сборника с научни трудове в съавторство с наши преподаватели, бе на симпозиуми в Потругалия и лятна школа в MIT – САЩ. През 2011 год. бе приета за студентка в този престижен университет [15, 16].

Въпреки че са изминали само четири години откакто е въведена учебната дисциплина „Компютърна стеганография”, могат да се направят някои изводи. За пръв път във висше учебно заведение у нас бе въведена учебна дисциплина, директно обучаваща по компютърна стеганология, с преобладаващ учебно – изследователски характер. Изградена е цялостна система за

обучение по дисциплината. Тя е изучавана от над 70 студенти от специалност Информатика (специализации „Компютърна информатика”, „Икономическа информатика”и „КИТ”) – редовно и задочно обучение. Разработени са над 15 бакалавърски и магистърски тези, обучават се докторанти, има над 18 съвместни статии и доклади, организирано е научно сътрудничеството с наши (УНИБИТ, НВУ, ВВМУ) и чуждестранни висши учебни заведения (Румъния, Русия, Украйна). Реализирани са проекти по стеганология, финансирани от фонд „Научни изследвания” на ШУ с участие на преподаватели, студенти и докторанти. Освен разработените стегопрограми и научни публикации, важен резултат е че постепенно се формира ново направление не само за ШУ – компютърна стеганология в паралелни компютърни среди.

Фиг. 2. *Колективът, разработил клъстерната система „Радиан-М”. На първия ред (отляво – надясно): проф. С. Желев, д-р Н. Николов, проф. С. Станев.*
На втория ред – д-р Ц. Цанков, д-р Т. Трифонов, д-р Д. Сърмов и д-р С. Железов.

Към учебната дисциплина има определен интерес от студентите в Шуменския университет и тя се избира от годината, в която е включена в учебните планове на трите специализации по специалността „Информатика”. По желание на студентите от специалностите „Национална сигурност” и „Комуникационно-информационни системи”, в дисциплините по компютърна сигурност са включени допълнително и теми по стеганография. Поради проявеният интерес и от колеги – преподаватели, първите резултати от обучението бяха докладвани на научни форуми [17, 18].

Развитието на компютърните технологии и мобилните комуникации неминуемо ще отправят нови предизвикателства към обучението на специалисти по високотехнологична стеганология, и те трябва да има готовност за тяхното посрещане. Ролята на висшите учебни заведения трябва да остане водеща в процеса на обучението и изследванията в тази област. Перспективно в създаването на учебно-изследователски клъстер, обхващащ университет, средно училище и софтуерни фирми, в който методите на стеганологията за защита на информацията ще заемат подобаващо им се място.

ЛИТЕРАТУРА

1. Станев, С. и С. Железов. Компютърна и мрежова сигурност. Университетско издателство “Епископ К. Преславски”, ЦДО, Шумен, 2005, ISBN 954-577-306-5, 132 стр.
2. Станев, С. и В. Галяев. Семантична еквивалентност на основните термини на компютърната стеганология в българските, английските и руските научни публикации. // Сборник научни трудове Международна научна конференция MATTEX2012, Шумен 2012. стр.119-126. ISSN 1314-3921.
3. Станев, С.,С. Железов, Т. Великова, В. Неделчева. За ефективността на стеганографските програми.//Сборник научни трудове. Научна конференция с межд.участие „40 години Шуменски университет”, Том ФМИ, Шумен, 2011.стр.97-102. ISBN 978-954-577-603-8.
4. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. ISBN 978-954-577-825-4.

5. Станев, С., С.Железов и Х. Параскевов. Компютърна стеганография. Методическо ръководство, VI част, Университетско издетелство "Епископ Константин Преславски", 2014 г., стр. 30 - 52 .
6. Железов, С. Оценка на ефективността на системи за защита на информацията в компютърните системи. Автореферат на дисертация за получаване на научно-образователна степен „доктор”. Шумен, ШУ „Еп.К.Преславски”, 2014.
7. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Информационные технологии и безопасность, Журнал Акад. наук Украины., Спец. выпуск, Киев, 2013, стр. 79-86.
8. Станев, С., С. Железов и И. Якимов. Реализация на паралелен стеганализ с клъстерна система.В: Сборник научни трудове Международна научна конференция „Съвременни методи и технологии в научните изследвания”, ИУ, Варна, 2012, стр.122-127. ISBN 978-954-21-0630-20.
9. Параскевов, Х. Методи за стеганографска защита на информация в компютърни мрежи. Автореферат на дисертация за получаване на научно-образователна степен „доктор”. Шумен, ШУ „Епископ К. Преславски”, 2014.
10. Кръстев, К. Повишаване на сигурността на участниците в мисии зад граница. Дисертация за получаване на научно-образователна степен „доктор”. София, УНИБИТ, 2014.
11. Станев, С., К. Кръстев. Стеганологична защита на информацията в контекста на контраразузнавателното осигуряване на сигурността на войскови контингент зад граница В: Сборник трудове на научна конференция „Новата парадигма за сигурност в киберпространството”. ФАПВОКИС на НВУ, Шумен, 2014 (под печат).
12. Stanev, S., H. Hristov and D. Dimanova. Aproaches for stegodefense of sensitive information. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. pp.117-122.
13. Станев, С. , Х. Христов и Д. Апостолов. Предизвикателства на компютърната и мрежова стеганография към дейността на фирмените служби за сигурност. Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.277-284. ISBN:978-954-535-796-1.
14. Zhelezov, S., H. Paraskevov, H. Hristov , P. Boyanov and B.Uzunova-Dimitrova. An architecture of staganological subsystem for information protection. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. pp.123-128.

15. Velcheva, K., S. Stanev and H. Paraskevov. Steganographic algorithms – research, analysis and implementation. In : Proceedings of CompSysTech, 2010.
16. Станев, С., К. Велчева, В. Велчева и Ст. Железов. Подход за стеганографско манипулиране на компютърни 3D виртуални обекти. В: Сборник трудове на научна конференция MATTEX2010, 2010.
17. Станев, С. и С. Железов. Первые результаты внедрения курса „Компютерная стеганография” в Шуменском университете. В: Трудове на международната научно-практическа конференция на ВДПУ „Коцюбински”, Виница, Украйна, 2012. стр.205-207.
18. Станев, С., С. Железов и Х. Параскевов Обучението по компютърна стеганография в Шуменския университет „Епископ Константин Преславски”. Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.445-451. ISBN 978-954-535-796-1.