Likholob Petr Georgiyevich, Assistant of the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russian Federation. E-mail: likholob@bsu.edu.ru

References

1. Alekseev A.P., Alenin A.A. Skrytaja peredacha dannyh v zvukovyh failah formata WAV [Hidden data transmission a sound file to wav format]. *Infokommunikacionnye tehnologii*, 2010, vol. 8, no. 3, pp.101-106.
2. Vercoe B.L. *Csound: A Manual for the Audio-Processing System*. MIT Media Lab, Cambridge, 1995.
3. Dutoit T., Marques F. *Applied Signal Processing A MATLAB TM-Based Proof of Concept*, Springer, 2009. 456 p.
4. Zhiljakov E.G. *Variacionnye metody analiza i postroenija funkcii po yempiricheskim dannym* [Variational methods of analysis and features from empirical data]. Belgorod, BelGU Publ., 2007. 160 p.
5. Zhiljakov E. G., Devicina C.N., Liholob P.G. Opredelenie vozmozhnogo ob''ema vnedrjaemoi informacii pri skrytoi peredache metok v rechevyh dannyh [Definition possible volume introduces information in secure communication tags in voice data]. *Nauchnye vedomosti BelGU. Serija «Informatika»,* 2012, no. 13, pp. 222-227.
6. Zhiljakov E.G. Belov S.P., Chernomorec A.A. Variacionnye metody analiza signalov na osnove chastotnyh predstavlenii [Variational methods of signal analysis based on frequency representation]. *Voprosy radioyelektroniki. Serija YeVT*, 2010, no. 1, pp. 10-26.
7. Ivanov M.A., CHugunkov I.V. Teorija, primenenie i ocenka kachestva generatorov psevdosluchainyh posledovatel'nostei [Theory, application and evaluation of the quality of pseudorandom sequence generator]. *Voprosy radioyelektroniki. Serija YeVT*, 2003, no. 1.

Received 20.05.2015

УДК 004.056

ТРЕБОВАНИЯ К УЧЕБНОЙ ЛИТЕРАТУРЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Алексеев А.П., Макаров М.И., Орлов В.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: apa_ivt@rambler.ru

Описываются требования к учебной литературе по криптографии и стеганографии, а также принципы построения современных систем защиты информации. Изучение методов защиты информации должно происходить путем решения большого числа практических задач. Описывается метод скрытого распределения информации по множеству каналов телекоммуникационной сети, причем в каждом канале используется оригинальный алгоритм защиты информации. Рассматривается метод сетевой стеганографии, заключающийся в сокрытии информации в значении длины сетевых пакетов.

Ключевые слова: криптография, стеганография, контейнеры, пространственно-временное распыление.

Введение

Число публикаций, посвященных криптографии и стеганографии, растет экспоненциально. По криптографии издано большое число учебников, задачников, пособий для проведения лабораторных работ и практических занятий [1-2; 12-13], а также проводятся онлайн курсы [10-11]. Применительно к стеганографии заметен дефицит учебной литературы, содержащей описание лабораторных работ и практических задач. Компенсировать это пробел пытаются преподаватели и ученые в различных высших учебных заведениях, в том числе России и Болгарии. В России такими работами являются [3-5], а в Болгарии - книги, написанные профессором С. Станевым и его учениками [6; 14-15].

Требования к учебной литературе

Авторы придерживаются мнения, что современная учебная литература по защите информа-

ции должна строиться на основе комплексного многоуровневого подхода. Это означает, в частности, что методы стеганографии невозможно рассматривать изолированно от криптографии. В свою очередь, рассмотрение только лишь криптографических алгоритмов защиты данных не раскрывает для студентов всей полноты современных методов обеспечения информационной безопасности. Несмотря на то что исторически стеганография появилась раньше, чем криптография, изложение материала в учебных пособиях целесообразно начинать именно с методов криптозащиты, поскольку теория криптографии разработана значительно глубже по сравнению со стеганографией.

Теоретическая часть учебного пособия должна содержать описание используемого математического аппарата. На наш взгляд, наибольшее внимание следует уделить модульной арифметике, булевой алгебре, математической статистике, теории вероятностей, спектральным преобразованиям (Фурье, дискретное косинусное преобразование) и теории искусственных нейронных сетей. Особое внимание нужно уделить Китайской теореме об остатках, теореме Байеса и алгоритму Евклида.

При изложении криптографических методов должны быть описаны методы замены, перестановок, гаммирования, алгоритмы шифрования с помощью открытых ключей. Здесь же целесообразно описать алгоритм цифровой подписи, хэш-функции и протоколы обмена ключами. Специалистам по защите информации приходится использовать случайные числа. Например, для псевдослучайного выбора адреса стеганографического внедрения или генерирования криптографического ключа. По этой причине в учебном пособии необходимо дать представление о достоинствах и недостатках различных алгоритмов формирования псевдослучайных чисел.

Так как нередко сокрытие данных происходит в мультимедийных контейнерах, то в теоретических разделах учебных пособий безусловно должны быть рассмотрены форматы контейнеров: графических, звуковых, текстовых, архивных, видео, Web-приложений. Скрывать передаваемые данные можно в любом электронном контейнере, обладающем избыточностью. Важно, чтобы студенты изучали материал по первоисточникам. Для этого в учебном пособии должны быть соответствующие литературные ссылки (на патенты, стандарты и технические спецификации). Обучаемые должны уметь количественно оценивать и сопоставлять по эффективности различные стеганографические и криптографические способы защиты информации.

Учебные пособия должны содержать материал, который многократно используется во многих алгоритмах защиты данных. Например, использование наименее значащих бит контейнера для сокрытия информации (метод LSB). В то же время студенты должны понимать, что рассматриваемые классические методы защиты информации не являются догмой и порой возможна их существенная модернизация. Так, внедрять информацию в звуковой файл формата WAV можно не только в младшие разряды цифровых отсчетов, но и в старшие разряды [7].

По нашему мнению, учебная литература должна содержать большое число примеров, которые позволят обучаемым понять идею метода защиты. Должны быть приведены программы, с помощью которых можно исследовать нюансы алгоритмов сокрытия информации. Для иллюстрации рассматриваемых идей можно использовать любой язык программирования или популярные математические системы. Предпочтение можно отдать языкам программирования C#, JavaScript, Java, Python и математическим системам Mathcad и MATLAB.

Не менее важным является развитие практических навыков. На лабораторных работах студенты должны познакомиться с современными достижениями криптографии и стеганографии (с опубликованными программами для сокрытия данных в мультимедийных файлах, например S-Tools). Работа с подобными программами позволяет обучаемым наглядно увидеть результаты сокрытия данных, невозможность органолептически (визуально или на слух) выявить секретное вложение. Очевидно, что обучаемые должны познакомиться с программами стеганоанализа (например, Stegdetect, Stego Suite, StirMark, Wireshark). Необходимо довести до сознания обучаемых, что возможна скрытая передача не только текста, но и произвольных данных (изображений, звуков).

Лучший способ освоения стеганографии – это выполнение лабораторных, курсовых работ, дипломных проектов и решение практических задач по извлечению скрытой в контейнерах информации. В этом случае необходимо познакомиться с редакторами памяти и сетевыми анализаторами. Объемные задачи по извлечению данных из электронных контейнеров вырабатывают у студентов пунктуальность и понимание того, что ошибка в одном бите часто приводит к катастрофическим последствиям. Сложные задачи приучают к дли-

тельному, напряженному, кропотливому труду, вырабатывают профессиональные навыки, необходимые будущим аналитикам. Сложные задачи создают убежденность в необходимости обязательного использования вычислительной техники, зачастую подталкивают к самостоятельному нахождению оригинальных способов решения задач.

Принципы построения современных систем защиты информации

Понятно, что наибольшее совершенствование своих навыков профессионалы могут получить, упражняясь в решении нестандартных задач стеганоанализа. В частности, для эффективного изучения стеганоанализа необходима как тренировка в применении уже известных статистических распределений в мультимедийных файлах, так и практика по формированию математических моделей контейнеров. Каждая книга пишется с учетом индивидуальных пристрастий авторов, она должна содержать оригинальные идеи, разработанные авторами. Тогда материал, полученный из первоисточника, представляет для обучаемых наибольший интерес.

Авторы статьи длительное время разрабатывают идею пространственно-временного распределения скрываемой информации. Предлагается использовать метод скрытого распределения информации по множеству каналов телекоммуникационной сети, что позволяет использовать идеи большого числа различных алгоритмов защиты информации. Следуя принципу многоуровневой защиты, распределяемая информация шифруется, стеганографически скрывается в контейнерах различной природы, применяется алгоритмический барьер в виде полного сцепления блоков защищаемых данных. Кроме того, информация распыляется не только в пространстве, но и во времени. Рассмотрим данный метод подробнее.

Корреспонденты связаны телекоммуникационной сетью. В их распоряжении имеется множество каналов связи. В текущем сеансе связи используются не все доступные каналы, а только их часть. Остальные каналы имитируют активность (передают служебную информацию, шум, дезинформацию). Камуфлирующие сообщения передаются по всем каналам. По каналам связи передаются стеганоконтейнеры. Такие каналы можно создать, например, с помощью протокола HTTP, FTP, электронной почты, ICQ, социальных сетей, интернет-радиостанций, интернет-TV и т.д. Для связи могут быть использованы локальные и глобальные сети. Сообщения целесообразно передавать не напрямую абоненту, а через промежуточные узлы и меняя на них протоколы. Корреспонденты обмениваются ключевой информацией и выбирают шифры А и В. Отправитель разбивает защищаемую информацию на блоки, зашифровывает их шифром А в режиме сцепления блоков. Затем полученная криптограмма разбивается на блоки большей длины и подвергается шифрованию по алгоритму В. Таким образом, получается криптограмма, каждый блок которой содержит несколько блоков криптограммы шифра А. Блоки криптограммы шифра В скрытно нумеруют и внедряют в них фрагменты ключа шифра А. С помощью стеганографического ключа определяют тип контейнера, параметры сокрытия и осуществляют внедрение битов криптограммы шифра В. Сформированные стего в соответствии со схемой организации и расписанием связи, определяемыми ключом распределения, передаются получателю.

На приемной стороне получатель накапливает поступающие контейнеры и в соответствии с ключом распределения извлекает информацию, применяя стеганографический ключ. Извлеченная криптограмма шифра В расшифровывается, при этом из ее блоков извлекаются фрагменты ключа шифра А. Наконец, расшифровав криптограмму шифра А с помощью составленного ключа, получают секретные данные. Достоинством многоуровневой защиты является возросшая сложность дешифрования криптограммы в случае отсутствия у криптоаналитика хотя бы одного блока криптограммы. Это происходит из-за необходимости многократного увеличения мощности вычислительных средств криптоаналитика. В данном методе если злоумышленник не смог перехватить блок криптограммы минимальной величины, то трудоемкость его вычислений увеличится в 264 раза [8].

Еще одна область интересов авторов – это сетевая стеганография. При рассмотрении этого направления защиты информации следует описывать не только привычные способы размещения бит секретной информации в специфичных для протокола полях заголовка, но и более современные способы защиты. Важным требованием является сокрытие данных при помощи ключа, определяющего позиции и порядок размещения бит секретной информации в контейнере. Одним из таких методов сетевой стеганографии является сокрытие информации в значении длины сетевого пакета.

Алгоритм сокрытия данных заключается в следующем. Для обмена информацией абонен-

ты выбирают симметричный ключ (одинаковый для сокрытия и извлечения). Отправитель вырабатывает на основании ключа двоичную криптографическую гамму. Используя двоичную гамму в качестве маски, отправитель располагает биты секретной информации в тех позициях (разрядах) значений длины сетевых пакетов, в которых биты маски равны единице, а на прочих местах, которым соответствуют нулевые биты маски, размещает случайные биты. Таким образом, формируется последовательность длин сетевых пакетов (точнее, длин данных, передаваемых в сетевых пакетах). Далее отправитель выбирает камуфлирующий текст, не несущий секретной информации, и посылает его в сеть пакетами в соответствии со сгенерированными длинами, включающими в себя биты секретной информации. В итоге в заголовках сетевых пакетов всех уровней отсутствуют сами биты секретной информации, однако опосредованно через фактическое значение длины камуфлирующих данных скрытно осуществляется передача секретных данных.

На приеме получатель действует симметрично: он накапливает камуфлирующий текст, поступающий из сети, одновременно запоминая длины пакетов. Формирует на основании ключа двоичную криптографическую гамму. Используя гамму в качестве маски, накладывает ее на значения длины поступивших сетевых пакетов и из позиций, соответствующих единичным битам гаммы, извлекает секретную информацию. Такой алгоритм может серьезно повлиять на эффективность использования канального ресурса и стать демаскирующим признаком для скрытого канала связи. Поэтому, договорившись заранее, абоненты могут принять несколько старших разрядов двоичного значения длины равными единице. Это решение позволяет передавать камуфлирующие данные на большей скорости, эффективнее используя канальный ресурс, и снизить вероятность обнаружения скрытого канала связи.

Важным требованием описанного алгоритма сокрытия данных является поддержание необходимой последовательности поступления пакетов на приемную сторону. При передаче пакетов по протоколу UDP может возникнуть ситуация, когда требующийся порядок поступления пакетов будет нарушен, что приведет к неверному извлечению скрытой информации. Для исключения этого недостатка отправитель и получатель должны разработать алгоритм восстановления последовательности пакетов либо применить протокол передачи, поддерживающий ее изначально, например TCP. Сложности технического характера могут возникнуть и при использовании протокола TCP, так как он предназначен для передачи потока информации без сохранения границ, то есть длин отдельных пакетов. Для решения этой проблемы может потребоваться собственная низкоуровневая реализация протокола TCP, работающая в обход средств операционной системы. Эти особенности позволяют сформулировать задачи для их проработки в рамках смежных дисциплин [9].

Выводы

Сформированное описанным образом учебное пособие позволяет получить теоретические сведения и практические навыки применения современных методов защиты информации. Погружение в методы криптографического и стеганографического анализа дает наглядное представление о сложности задач защиты информации, стимулирует итерационное развитие методов защиты данных.

Литература

1. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. М.: Гелиос АРВ, 2004. – 144 с.
2. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. СПб: БХВ-Петербург, 2007. – 304 с.
3. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации: учебное пособие. Самара: Изд-во ПГУТИ, 2010. – 330 с.
4. Алексеев А.П. Информатика для криптоаналитиков: учебное пособи. Самара: Изд-во ПГУТИ, 2015. – 376 с.
5. Алексеев А.П. Информатика 2015. М.: СОЛОН-Пресс, 2015. – 400 с.
6. Станев С.С. Стеганологична защита на информацията. Университетско издателство «Епископ Константин Преславски». Шумен, 2013. – 320 с.
7. Аленин А.А., Алексеев А.П. Помехоустойчивое стеганографическое внедрение информации в звуковые файлы // Вопросы защиты информации. №1, 2013. – С. 15-19.
8. Патент RU 2462825. Способ скрытой передачи зашифрованной информации по множеству каналов связи / Алексеев А.П., Макаров М.И. Заявл. 08.07.2011; опубл. 27.09.2012, бюл. №27.
9. Орлов В. В., Алексеев А. П. Активная скрытая передача информации в сетях TCP/IP // Тезисы докладов Шестой Международной научно-

технической конференции «Проблемы техники и технологии телекоммуникаций». – 2008, Казань. – 25 – 27 ноября 2008 г., с. 446-447.
10. Cryptography I – Coursera // URL: https://www.coursera.org/course/crypto (д.о. 9.06.2015).
11. Applied Cryptography and Encryption Class Online – Udacity // URL: https://www.udacity.com/course/cs387 (д.о. 9.06.2015).
12. Paar C., Pelz, J. Understanding Cryptography Springer, 2010. – 372 p.
13. Junod P. A Classical Introduction to Cryptography Exercise Book. Springer Science & Business Media, 2005. – 254 c.
14. Станев С., Железов С., Параскевов Х. Обучението по компютърна стеганография в Шуменския университет «Епископ Константин Преславски». Наука, образование, сигурност. София: Издателство на НБУ, 2013. – С. 445-451.
15. Станев С., Железов С. Первые результаты внедрения курса «Компютерная стеганография» в Шуменском университете // Трудове на международната научно-практическа конференция на ВДПУ «Коцюбински». Украина, Винница, 2012. – С. 205-207.

Получено 26.06.2015

Алексеев Александр Петрович, к.т.н., доцент, профессор Кафедры информатики и вычислительной техники (ИВТ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел.: 8 (846) 2280057. E-mail: apa_ivt@rambler.ru

Макаров Максим Игоревич, к.т.н., доцент Кафедры ИВТ ПГУТИ. Тел. 8-902-323-61-12. E-mail: moox700@gmail.com

Орлов Владимир Владимирович, к.т.н., ведущий инженер-программист ЗАО «Самарский булочно-кондитерский комбинат». Тел. 8-927-704-10-30. E-mail: crypterus@yandex.ru

DATA PROTECTION EDUCATIONAL MATERIAL REQUIREMENTS

Alekseev A.P., Makarov M.I., Orlov V.V.
Povolzhskiy State University of Telecommunication and Informatics, Samara, Russian Federation
E-mail: apa_ivt@rambler.ru

This article is devoted to data protection educational material requirements. Here we describe modern data protection principles, selection guideline for application-oriented programming language and mathematical system, the necessity of applying network analyzers and memory editors, and criterions to information security problems. Multi-layer information security consideration combines studying of cryptography and steganography algorithms. We propose to use the method for hidden distribution of information over set of telecommunication network channels, which provides to apply data protection original algorithm for each particular channel. According to multi-layer information security principles, distributed information is encrypted and it is hidden steganographically over different kinds of containers. Here algorithmic barrier is utilized as a complete linkage of protected data blocks. Moreover this information diffuses not only spatially but also in time. Also we describe a method for network steganography based on information hiding over length of network packet.

Keywords: cryptography, steganography, containers, spatiotemporal diffusion

DOI: 10.18469/ikt.2015.13.3.15

Alekseev Aleksander Petrovich, PhD in Technical Science, Professor of Department of Information and Computer Engineering, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel. +78462280057. E-mail: apa2008@rambler.ru.
Makarov Maxim Igorevich, PhD in Technical Science, Assistant Professor of Department of Information and Computer Engineering, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel.: +79023236112. E-mail: moox700@gmail.com
Orlov Vladimir Vladimirovich, PhD in Technical Science, Principal Software Engineer, CJSC "SBKK", Samara, Russian Federation. Tel.: + 79277041030. E-mail: crypterus@yandex.ru

References

1. Osipyan V.O., Osipyan K.V. *Kriptografiya v zadachax i uprazhneniyax* [Cryptography problems and exercises]. Moscow, Gelios ARV Publ., 2004. 144 p.
2. Moldovyan N.A. *Praktikum po kriptosistemam s otkrytym klyuchom* [Workshop on publickey cryptosystems]. St. Petersburg, BXV-Peterburg Publ., 2007. 304 p.
3. Alekseev A.P., Orlov V.V. *Steganograficheskie i kriptograficheskie metody zashchity informatsii: uchebnoe posobie* [Steganographic and cryptographic methods of information protection]. Samara, PSUTI Publ., 2010. 330 p.
4. Alekseev A.P. *Informatika dlya kriptoanalitikov: uchebnoe posobie* [Informatics for cryptanalysts]. Samara, PSUTI Publ, 2015. – 376 p.
5. Alekseev A.P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p.
6. Stanev S. *Steganologichna zashhita na informacijata*. Universitetsko izdatelstvo «Episkop Konstantin Preslavski». Shumen, 2013. 320 p. (In Bulgarian).
7. Alenin A.A., Alekseev A.P. Pomexoustojchivoe steganograficheskoe vnedrenie informacii v zvukovy'e fajly [Interference steganography introduction of information into audio files]. *Voprosy zashhity informacii,* 2013, no. 1, pp. 15 – 19.
8. Alekseev A.P., Makarov M.I. Pat. RF. *Sposob skrytoi peredachi zashifrovannoi informatsii po mnozhestvu kanalov svyazi* [Method of secure data transmission of encrypted information over multiple communication channels]. Patent RF, no. 2462825, 2012.
9. Orlov V.V., Alekseev A.P. *Aktivnaya skrytaya peredacha informatsii v setyakh TCP/IP* [Active secure communication in networks TCP / IP.]. *Tezisy dokladov Shestoi Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii «Problemy tekhniki i tekhnologii telekommunikatsii 2008»*, Kazan, 2008, pp. 446-447.
10. Cryptography I – Coursera. Available at: https://www.coursera.org/course/crypto. (accessed 9.06.2015).
11. Applied Cryptography and Encryption Class Online - Udacity. Available at: https://www.udacity.com/course/cs387. (accessed 9.06.2013).
12. Paar. C., Pelzl, J. *Understanding Cryptography*. Springer, 2010. 372 p.
13. Junod P. *A Classical Introduction to Cryptography Exercise Book.* Springer Science & Business Media, 2005. 254 p.
14. Stanev S., Zhelezov S., Paraskevov X. *Obuchenieto po kompyuturna steganografiya v Shumenskiya universitet «Episkop Konstantin Preslavski». Nauka, obrazovanie, sigurnost.* Sofiya, Izdatelstvo na NBU, 2013, pp. 445-451. (In Bulgarian).
15. Stanev S., Zhelezov S. Pervye rezul'taty vnedreniya kursa «Kompyuternaya steganografiya» v Shumenskom universitete [The first results of the implementation of the course «Computer steganography» in Shoumen University]. *Trudove na mezhdunarodnata nauchno-prakticheska konferenciya na VDPU «Kocyubinski»,* Vinnica, Ukraina, 2012, pp. 205 – 207.

Reseived 26.06.2015

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 004.65:378

УПРАВЛЕНИЕ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВУЗА

Болодурина И.П., Волкова Т.В., Ащеулова Н.А.
Оренбургский государственный университет, Оренбург, РФ
E-mail: prmat@mail.osu.ru

В статье рассматриваются вопросы управления правами доступа пользователей корпоративной автоматизированной информационной системы (КАИС) вуза в целях назначения субъекту доступа минимально необходимых привилегий. Представлена модель политики управления доступом, соединяющая ограничения предметной области и мандатной политики доступа СУБД Oracle. Модель позволяет гибко реагировать на изменения принадлежности субъекта и объекта доступа к тем или иным узлам иерархии подчинения подразделений вуза и внедрена в рамках проекта «Информационно-аналитическая система Оренбургского государственного университета».