МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Монография

Харьков, 2015

УДК 681.518.54
ББК 32.965
И74

Рекомендовано на заседании ученого совета Харьковского национального экономического университета имени Семена Кузнеца (протокол № 9 от 30.03.2015 г.)

Рецензенты:

Сопронюк Федор Алексеевич – доктор физико-математических наук, профессор, зав. кафедрой математических проблем управления и кибернетики, Черновецкий национальный университет имени Юрия Федьковича;

Кораблев Николай Михайлович – доктор технических наук, профессор кафедры ЭВМ, ХНУРЭ;

Хома Владимир Васильевич – доктор технических наук, профессор кафедры "Защита информации", НУ "Львовская политехника".

И74 Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под ред. В.С. Пономаренко. – Х. : Вид. ТОВ “Щедра садиба плюс”, 2015. – 486 с., Русск. яз.
ISBN 978-617-7225-03-3

В монографии рассмотрены результаты исследований использования информационных систем и применения информационных технологий для решения широкого круга задач в управлении, образовании, экономике, промышленности, современные подходы решения задач обеспечения услуг безопасности и скрытности данных, циркулирующих в коммуникационных системах.

Монография представляет интерес как для специалистов сферы IT-технологий, обеспечения услуг безопасности и передачи в коммуникационных системах, управлением программами информатизации компаний, так и для более широкого круга преподавателей, аспирантов, студентов, специализирующимся в области разработки информационных систем и IT-технологий, полиграфии, защиты и передачи данных.

У монографії розглянуті результати досліджень використання інформаційних систем і застосування інформаційних технологій для вирішення широкого кола завдань в управлінні, освіті, економіці, промисловості, сучасні підходи вирішення завдань забезпечення послуг безпеки і скритності даних, що циркулюють в комунікаційних системах.

Монографія представляє інтерес як для фахівців сфери IT-технологій, забезпечення послуг безпеки та передачі в комунікаційних системах, управлінням програмами інформатизації компаній, так і для більш широкого кола викладачів, аспірантів, студентів, що спеціалізуються в області розробки інформаційних систем та IT-технологій, поліграфії, захисту і передачі даних.

УДК 681.518.54
ББК 32.965
ISBN 978-617-7225-03-3

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

Информационные технологии в экономике, экологии, медицине и образовании

Стартапы и инновационное предпринимательство

СОДЕРЖАНИЕ

Компьютеризированные технологии и системы издательско-полиграфических производств и электронных мультимедийных изданий

ВВЕДЕНИЕ

Современный этап развития и внедрения современных информационно-коммуникационных технологий характеризуется расширением и развитием сферы их использования. Это относится к таким направлениям, как автоматизация технических и социально-экономических систем, образование и наука, промышленное производство. Важнейшими вопросами, требующими своего решения, является внедрение информационных систем и технологий в сферах, определяемых государственными программами приоритетных направлений науки и техники и образования. В этой связи актуальность разработки новых концепций, подходов и методов, позволяющих повысить эффективность функционирования современных информационных систем, является актуальной.

Данная монография отражает научные исследования, посвященные различным аспектам информационных систем и технологий, представленным на VII Международной научно-практической конференции “Проблемы и перспективы развития IT-индустрии”, проведенной на базе кафедры информационных систем Харьковского национального экономического университета имени Семена Кузнеца 17–18 апреля 2015 г.

В монографии нашли отражение результаты научных исследований в сфере применения информационных технологий в технических системах, защиты информации в информационно-коммуникационных системах, использования информационных технологий в экономике, экологии, медицине и образовании, в компьютеризированных технологиях и издательско-полиграфических производствах и электронных мультимедийных изданий, проблематике стартапов и инновационного предпринимательства.

В разделах 1 – 6 приведены основные результаты, представленные на секции 1 “Информационные технологии в технических системах”:

проведен анализ эффективности алгоритмов маршрутизации пакетов в сетях, использующих гибридные протоколы; рассмотрена эффективность применения фибоначчи-подобных систем счисления; предложен и исследован метод управления доступом в интеллектуальных узлах коммутации; разработана структура базы данных интегрированной информационной системы; исследованы методы и процедуры проектирования тестовых наборов на основе упорядоченных каскадных таблиц решений; проведен синтез совмещенной лазерной системы связи с кооперирумыми летательными аппаратами.

В разделах 7 – 20 отражены основные результаты, представленные на секции 2 “Защита информации в информационных коммуникационных системах”:

рассмотрены рандомизированные криптографические примитивы нелинейной подстановки; рассмотрены концептуальные основы безопасности информационно-коммуникационных технологий; рассмотрен усовершенствованный алгоритм MAC, основанный на использовании модулярных преобразовани; проведено исследование угроз методов двухфакторной аутентификации; рнассмотрен метод восстановления параметров объектов информационного обеспечения автоматизированных систем управления на основе дифференциально-нетейлоровских преобразований; расмотрены принципы мониторинга информационной инфраструктуры при обеспечении миграции данных в безопасные сегменты; разработаны общие принципы построения методов выявления нарушения целостности цифрового изображения; предложены подходы к повышению производительности операции деления больших целых чисел на основе расширенного алгоритма Евклида; разработана модель системы информационной безопасности консолидированной информации при информационном противоборстве; разработаны стеганографические методы и алгоритмы, устойчивые к атаке сжатием, а также методика их сравнительной оценки; предложены стратегия, методы и модели управления безопасностью информационных технологий; рассмотрены конечные поля, порождаемые пространственными матрицами Галуа; разработаны подходы к повышению производительности операции деления больших целых чисел, на основе расширенного алгоритма Евклида.

В разделах 21 – 26 отражены основные результаты, представленные на секции 3 «Информационные технологии в экономике, экологии, медицине и образовании»:

разработана технологическая платформа, как инновационный элемент развития предприятий машиностроительной отрясли;

разработаны организационные и технологические модели дистанционного обучения в правовых дисциплинах; проведено моделирование поведения участников канала сбыта на основе аппарата сетей Петри; разработано математическое и программное обеспечение задачи проектирования и модернизации организационной структуры управления агрохолдингом; разработаны модели и информационные технологии управления конкурентоспособностью промышленного предприятия.

В разделе 27 отражены результаты, представленные на секции 4 «Стартапы и инновационное предпринимательство»: разработка метода минимизации объема передачи данных в системах онлайн-поддержки стартап-проектов.

В разделах 28 – 33 отражены основные результаты, представленные на секции 5 «Компьютеризированные технологии и системы издательско-полиграфических производств и электронных мультимедийных изданий»:

разработана методика разработки web-приложения для приёма заказов оперативной полиграфии; разработана методика количественной оценки связей между критериями качества мультимедийной продукции; разработана методика разработки web-портала полиграфических дисциплин; проведен анализ методов сжатия изображений оцифрованного текста; разработан метод компрессии изображения текста на основе нечеткой классификации вертикальных элементов строки; разработана системв поддержки принятия стратегических решений по управлению полиграфическими предприятиями в условиях технологической революции.

Монография предназначена для научных работников и профессорско-преподавательского состава высших учебных заведений, работающих в сфере информационно-коммуникационных технологий.

Монография подготовлена авторским коллективом в следующем составе:

1. Алёшин Г.В., Украинская государственная академия железнодорожного транспорта, доктор технических наук, профессор кафедры транспортной связи– раздел 6 (в соавторстве);
2. Белецкий А.Я., Национальный авиационный университет, доктор технических наук – раздел 7, 20;
3. Биккузин К.В., Харьковский национальный экономический университет имени Семена Кузнеца, преподаватель кафедры информационных систем.– раздел 9 (в соавторстве);
4. Бондарь И.А., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат экономических наук, доцент кафедры компьютерных систем и технологий – раздел 28 (в соавторстве);
5. Браткевич В. В., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, профессор кафедры компьютерных систем и технологий – раздел 29;
6. Брынза Н.А., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, доцент кафедры ИКТ – раздел 21, 22 (в соавторстве);
7. Вильхивская О.В., Харьковский национальный экономический университет имени Семена Кузнеца, преподаватель – раздел 21, 22 (в соавторстве);
8. Гвозденко М.В., Национальный юридический университет имени Ярослава Мудрого, старший преподаватель – раздел 31 (в соавторстве);
9. Грабовский Е.Н., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат экономических наук, доцент кафедры компьютерных систем и технологий – раздел 30 (в соавторстве);

10. Дудыкевич В.Б., Национальный университет "Львовкая политехника", доктор технических наук, профессор, заведующий кафедры защиты информации – раздел 8 (в соавторстве);

11. Евсеев С.П., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, доцент кафедры информационных систем – раздел 10 (в соавторстве);

12. Засядько А.А., Черкасский институт банковского дела Университета банковского дела Национального банка Украины, доктор технических наук, профессор кафедры высшей математики и информационных технологий – раздел 11;

13. Иванов В.Г., Национальный юридический университет имени Ярослава Мудрого, доктор технических наук, профессор – раздел 31 (в соавторстве);

14. Иванов С.Н., Национальный юридический университет имени Ярослава Мудрого, кандидат технических наук, доцент – раздел 23 (в соавторстве);

15. Казакова Н.Ф., Одесский национальный экономический университет, кандидат технических наук, доцент кафедры информационных систем в экономике – раздел 12 (в соавторстве);

16. Карасюк В.В., Национальный юридический университет имени Ярослава Мудрого, кандидат технических наук, доцент – раздел 23 (в соавторстве);

17. Кобозева А.А., Одесский национальный политехнический университет, доктор технических наук, профессор – раздел 13;

18. Коваленко А.В. – Кировоградский национальный технический университет, кандидат технических наук, доцент кафедры программного обеспечения – раздел 4 (в соавторстве);

19. Коваленко А.С., Кировоградский национальный технический университет, ассистент кафедры программного обеспечения – раздел 4 (в соавторстве);

20. Ковтун В.Ю., Национальный авиационный университет, кандидат технических наук, доцент кафедры безопасности информационных технологий – раздел 14, 15 (в соавторстве);

21. Ковтун М.Г., Национальный авиационный университет, аспирант кафедры безопасности информационных технологий – раздел 15 (в соавторстве);

22. Коломийцев А.В., Харьковский университет Воздушных Сил им. Ивана Кожедуба, кандидат технических наук, начальник научно-исследовательского отдела научного центра ВС ХУВС им. Ивана Кожедуба, Заслуженный изобретатель Украины – раздел 6 (в соавторстве);

23. Кононович В.Г., Одесский национальный политехнический университет, кандидат технических наук, доцент – раздел 16 (в соавторстве);

24. Кононович И.В., Одесская национальная академия пищевых технологий, аспирант – раздел 16 (в соавторстве);

25. Король О.Г., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, доцент кафедры информационных систем – раздел 9 (в соавторстве);

26. Коц Г.П., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат экономических наук, доцент кафедры информационных систем – раздел 28 (в соавторстве);

27. Кошевая Н.А., Национальный юридический университет имени Ярослава Мудрого, кандидат технических наук, доцент – раздел 17 (в соавторстве);

28. Ломоносов Ю.В., Национальный юридический университет имени Ярослава Мудрого, кандидат технических наук, доцент кафедры информатики и вычислительной техники – раздел 32 (в соавторстве);

29. Лосев М.Ю. Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, доцент кафедры информационных систем – раздел 1;

30. Лысенко И.А., Кировоградский национальный технический университет, аспирант – раздел 5 (в соавторстве);

31. Любарский М.Г., Национальный юридический университет имени Ярослава Мудрого, доктор физ. – матем. наук, профессор кафедры информатики и вычислительной техники – раздел 32 (в соавторстве);

32. Мазниченко Н.И. Национальный юридический университет имени Ярослава Мудрого, старший преподаватель – раздел 17 (в соавторстве);

33. Максимович В.Н., Национальный университет "Львовкая политехника", доктор технических наук, заведующий кафедры БИТ – раздел 8 (в соавторстве);

34. Манева Р.И., Национальный технический университет «Харьковский политехнический институт», аспирант – раздел 25 (в соавторстве);

35. Мельник М.А., Одесский национальный политехнический университет, кандидат технических наук, доцент кафедры информационная безопасность – раздел 18;

36. Микитин Г.В., Национальный университет "Львовкая политехника", доктор технических наук, профессор кафедры защиты информации, – раздел 8 (в соавторстве);

37. Мохамад Абу Таам Гани, Кировоградский национальный технический университет, аспирант – раздел 3 (в соавторстве);

38. Охрименко А.А., Национальный авиационный университет, ассистент кафедры безопасности информационных технологий – раздел 14 (в соавторстве);

39. Петришин Л.Б., AGH University of Science and Technology, Прикарпатский национальный университет им. В. Стефаника, доктор технических наук, заведующий кафедры информатики – раздел 2 (в соавторстве);

40. Петришин М.Л., Прикарпатский национальный университет им. В. Стефаника, аспирант – 2 (в соавторстве);

41. Потрашкова Л.В., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат экономических наук, доцент кафедры компьютерных систем и технологий – раздел 33;

42. Пушкарь А.И., Харьковский национальный экономический университет имени Семена Кузнеца, доктор экономических наук, профессор, заведующий кафедры компьютерных систем и технологий – раздел 30 (в соавторстве);

43. Свердло Т.А., Харьковский национальный экономический университет имени Семена Кузнеца, преподаватель кафедры информационных систем – раздел 10 (в соавторстве);

44. Смирнов А.А., Кировоградский национальный технический университет, доктор технических наук, заведуюший кафедры программного обеспечения – раздел 3, 5 (в соавторстве);

45. Ушакова И.А., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат экономических наук, доцент кафедры информационных систем – раздел 24;

46. Фонта Н.Г., Национальный технический университет «Харьковский политехнический институт», кандидат технических наук, доцент – раздел 26 (в соавторстве);

47. Фразе-Фразенко А.А., Одесский национальный экономический университет, заместитель начальника центра информационных технологий – раздел 12 (в соавторстве);

48. Хорошко В.А., Национальный авиационный университет, доктор технических наук, профессор – раздел 19 (в соавторстве);

49. Хохлачова Ю.Е., Национальный авиационный университет, старший преподаватель – раздел 19 (в соавторстве);

50. Шматко А.В., Национальный технический университет «Харьковский политехнический институт», кандидат технических наук, доцент – раздел 25, 26 (в соавторстве);

51. Щербаков А.В., Харьковский национальный экономический университет имени Семена Кузнеца, кандидат технических наук, профессор кафедры информационных систем – раздел 27;

Кафедра информационных систем Харьковского национального экономического университета имени Семена Кузнеца выражает благодарность всем исследователям, принявшим участие в подготовке и публикации монографии.

РАЗДЕЛ 17
ИСПОЛЬЗОВАНИЕ СТЕНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ

Аннотация. *В работе рассматриваются задачи, решаемые в рамках систем защиты информации, особое место среди которых занимает задача специального кодирования информации в виде данных, предназначенных для скрытой передачи информации, называемая задачей стеганографии. Проведен обзор методов и алгоритмов текстовой стеганографии, применяющихся в сфере защиты авторских прав.*

Ключевые слова: *Стеганография, стегоанализ, лингвистические стегосистемы, текстовая стеганография*.

Abstract. *This article contains problems, which are solved in boundaries of information protection systems, where special coding of information in form of data for concealed delivery, plays an essential role. It is called steganography. A review shows some methods and algorithms of text steganography that are used in the field of copyright protection*.

Keywords: *Steganography, steganalysis, linguistic stegosystem, text steganography.*

Введение и постановка задачи. Бурное развитие информационных технологий, которое наблюдается в последние годы, привело к тому, что сегодня огромное количество информации, составляющей интеллектуальную собственность, хранится и обрабатывается в компьютерных сетях и/или распространяется в цифровой форме.

Наиболее распространенными нарушениями прав интеллектуальной собственности сегодня являются пиратство, плагиат, подделка информации, изменение информации, недобросовестная конкуренция (промышленный шпионаж и т. п.).

При этом наибольшее внимание уделяется защите прав интеллектуальной собственности мультимедийной информации, распространяемой на цифровых носителях и в сети Интернет, однако упор делается больше на правовое решение проблемы, технические вопросы остаются на втором плане. В то же время нельзя забывать о том, что огромное количество информации представлено в обычном текстовом виде: книги, статьи, электронная переписка, документы, отчеты и многое другое. Причем в области электронного документооборота технические вопросы защиты интеллектуальной собственности не могут быть полностью решены только лишь стандартными средствами защиты информации.

Среди задач, решаемых в рамках систем защиты, особое место занимает задача специального кодирования информации в виде данных, предназначенных для скрытой передачи информации, называемая задачей стеганографии. Построение стеганографических методов привлекает внимание многих специалистов, занятых разработкой новых технологий (например, технологий анализа и фильтрации передаваемой информации в сети), направленных на обеспечение высокой надежности информационных систем. В целом задача

стеганографии и противоположная ей задача стегоанализа являются одними из базовых проблем в теории надежности и безопасности информационных технологий. В отличие от криптографии, ограничивающей доступ к информации, содержащейся в передаваемом сообщении с помощью некоторого секретного ключа, задача стеганографии состоит в том, чтобы скрыть сам факт передачи какого-либо сообщения от третьих лиц. Обычно, такая задача решается путем внедрения передаваемого секретного сообщения в безобидный на вид объект данных, так называемый контейнер. Сам контейнер подбирается таким образом, чтобы факты его существования или передачи не вызывали никакого подозрения. Основными характеристиками методов стеганографии следует считать объем внедряемого сообщения и устойчивость к анализу (обнаружению факта наличия внедрения).

В цифровой стеганографии в качестве контейнера используется цифровой объект – компьютерный файл. Современные методы встраивания позволяют внедрять скрытую информацию в файлы аудио, видео, текста, исполняемых программ и т.д. В настоящее время существует большое количество стеганографических программных пакетов как коммерческих, так и бесплатных, с графическим интерфейсом и в виде консольных приложений.

Цифровая стеганография получила широкое применение в сфере защиты авторских прав. В объект авторского права может быть внедрена специальная метка – отпечаток пальца (fingerprint), которая идентифицирует законного получателя. Например, в каждую продаваемую копию программы может быть внедрена метка, идентифицирующая лицензионного покупателя. В случае обнаружения пиратской копии программы при помощи встроенной метки без труда может быть отслежен пользователь, нарушивший лицензионное соглашение. Еще одной встраиваемой меткой может быть цифровой водяной знак (ЦВЗ, watermark), идентифицирующий автора. Предположим, в фотографию внедряется специальная метка, содержащая паспортные данные автора. Затем обнаруживается постороннее лицо, выдающее эту фотографию как свою собственную. В ходе судебного разбирательства с помощью извлеченного водяного знака может быть установлен истинный автор фотографии. Менее проработанным является вопрос защиты текстовой информации при помощи внедрения ЦВЗ. В литературе можно встретить описание синтаксических и семантических методов внедрения информации, однако отсутствует их адаптация для внедрения ЦВЗ.

Скрываемая информация называется стеганограммой или просто стего. Данные, среди которых она прячется, играют роль информационного контейнера, а потому так же и именуются. Для компьютерного вируса, например, контейнером служит исполняемый файл. Одна и та же стеганограмма может быть упакована в различные контейнеры подобно тому, как одна и та же криптограмма шифруется различными методами или ключами. Если продолжить сравнение с

вирусами, то аналогом криптограммы являются обитающие в вычислительной среде компьютерные черви, не нуждающиеся ни в каком носителе.

Тем не менее, некоторые авторы не склонны придавать значение собственной информации контейнера, считая ее безразличной как для отправителя, так и для получателя стегосообщения [140]. Однако это не совсем так, что подтверждается все тем же примером компьютерного вируса.

Контейнером могут служить любые данные (файлы) достаточно большого объема, например, графические или звуковые. Их структура проста и, как правило, обладает большой избыточностью, позволяющей вместить значительный объем дополнительной информации. Однако текстовые файлы все же более распространены, и их структура широко известна. Стеганография, использующая текстовые контейнеры, называется текстовой (text steganography).

В настоящее время проводится множество конференций, по проблемам информационной безопасности. С каждым годом растет число публикаций, посвященных методам стеганографии и стегоанализа. В этом направлении науки работают такие ученые, как: В.Г. Грибунин, И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов, Р. Бергмар (R. Bergmar), К. Качин (C. Cachin), М. Чапман (M. Chapman), Ж. Чень (J. Chen), Д. Фридрич (J. Fridrich), и др.

В то же время, вопросам текстовой стеганографии посвящено сравнительно мало работ. Авторами проведен анализ основных отечественных и зарубежных источников за более чем 10 последних лет. Целью работы является обзор методов и алгоритмов текстовой стеганографии и стегоанализа, применяющихся в сфере защиты авторских прав, анализ надежности и безопасности использования информационных технологий, базирующихся на этих методах.

Основная часть. На сегодняшний день существует множество способов встраивания скрытой информации в тестовые файлы. Их можно условно разделить на следующие группы: синтаксические методы, лексические методы (лингвистическая стеганография) и мимикрия (mimic-function — методы имитирующих функций).

Синтаксические методы основаны на использовании особенностей пунктуации, аббревиатуры и сокращения. Хотя правила пунктуации достаточно строго оговорены правилами используемого языка, существуют случаи, когда эти правила оказываются неоднозначными или же отклонение от них, не ведет к существенному искажению смысла скрывающего текста. К синтаксическим методам относят также методы, основанные на изменении стиля и структуры предложения без заметного искажения исходной смысловой нагрузки.

При использовании синтаксических методов в текстовых файлах секретная информация чаще всего кодируется путем изменения количества пробелов, использования невидимых символов, регистра букв, путем изменения межстрочных интервалов, табуляций и т д. Синтаксические конструкции легко встраиваются в любой текст, независимо от его содержания, назначения и языка.

Такие системы легко разрабатывать и выполняются они автоматически. Но они легко взламываются, и секретная информация легко устраняется путем простейших атак.

В рукописном тексте написание отдельных символов может заметно варьироваться, помимо явных различий в начертании символов, может отличаться высота букв, их ширина, высота средней линии, угол наклона и т. д. Все это может эффективно использоваться для передачи скрытых посланий. Основная сложность методов, основанных на использовании особенностей символов, заключается лишь в формировании правил различения буквы открытого текста от аналогичной буквы скрытого сообщения. В простейшем случае, возле отдельных букв могут встречаться "случайные" точки или едва заметные подчеркивания. Поскольку символы текста в электронном виде идентичны, для целей цифровой стеганографии данный подход малоприменим.

В основу методов кодирования смещением строк положено изменение интервала между строками сообщения. Каждая строка маскирующего текста сдвигается немного вверх или вниз относительно своего исходного положения (базовой линии), соответственно смещением строки вверх можно закодировать, например, единицу, а вниз ноль очередного двоичного символа скрываемого сообщения. Так же может использоваться и сам межстрочный интервал. Метод достаточно часто применяется для целей скрытой маркировки твердых копий электронных документов при печати на сетевых принтерах.

Кодирование с использованием изменения горизонтального интервала между отдельными словами или символами наиболее эффективно при выборе в качестве маскирующего сообщения больших текстов с выравниванием по ширине, так как в данном случае расстояние между словами может меняться в достаточно широких пределах. В ряде случаев применяется кодирование не только длиной символов пробела, но и их числом. Так, два пробела в интервале между предложениями могут кодировать очередной двоичный символ скрытого сообщения со значением, равным единице, а один – со значением нуля. Аналогично могут быть использованы пробельные символы в конце строки.

Достаточно полная классификация подобных методов приведена в работе [34]. Удивление вызывает лишь тот факт, что из автоматических методов текстовой стеганографии в этой статье упомянут только один – выравнивание текста с помощью пробелов.

Суть данного метода состоит в раздвижке строки путем увеличения пробелов между словами, когда один пробел соответствует, например, биту 0, два пробела – биту 1. Однако прямое его применение хотя и возможно, но на практике порождает массу неудобств, в частности, оформление текста становится неряшливым, что позволяет легко заподозрить в нем наличие стега.

В работе [2] приведена программа, где подобные проблемы уже решены. Программа попросту перераспределяет пробелы в пределах текущей длины

строки, перенося по возможности длинные пробелы в ее конец. В результате строки выходного текста имеют аккуратный вид, затрудняющий выявление стега.

Одиночные пробелы и пробелы перед последним словом строки не несут информационной нагрузки. В остальных случаях же четное число пробелов кодирует 0, нечетное – 1. Стега при записи предварительно шифруется, а при чтении расшифровывается с использованием операции исключающего «ИЛИ» и встроенного в систему программирования датчика случайных чисел, управляемого константами Key1 и Key2.

Программа работает в двух режимах, определяемых числом параметров вызова. Первым параметром всегда указывается текстовый файл контейнера. Если таких параметров два, программа извлекает стега из контейнера и помещает его в файл, указанный вторым параметром. Параллельно стега распечатывается на экране. При трех параметрах происходит создание стега. Источником стегосообщения является файл, указанный вторым параметром, а результат работы программы помещается в файл, заданный третьим.

Необходимость учета множества нюансов делает данную программу довольно сложной. Поэтому представляют интерес другие способы встраивания стегосообщения. Из всех таких способов были выбраны простейшие. Если перечислять их с повышением уровня сложности, то это будет метод изменения порядка следования маркеров конца строки, метод хвостовых пробелов, метод знаков одинакового начертания и метод двоичных нулей. Теперь кратко рассмотрим их.

Метод изменения порядка следования маркеров конца строки CR/LF использует индифферентность подавляющего числа средств отображения текстовой информации к порядку следования символов перевода строки (CR) и возврата каретки (LF), ограничивающих строку текста. Традиционный порядок следования CR/LF соответствует 0, а инвертированный LF/CR означает 1.

Метод хвостовых пробелов предполагает дописывание в конце коротких строк (менее 225 символов; значение 225 выбрано достаточно произвольно) от 0 до 15 пробелов, кодирующих значение полубайта.

Метод знаков одинакового начертания предполагает подмену (бит 1) или отказ от такой подмены (бит 0) кириллического символа латинским того же начертания.

Метод двоичных нулей является разновидностью метода знаков одинакового начертания и предполагает либо замену первого в группе из двух или более внутренних пробелов двоичным нулем (бит 1), либо отказ от нее (бит 0).

Интерфейс программ одинаков. Всего возможны три режима их работы, определяемые числом параметров вызова, первый из которых всегда представляет файл стеганоконтейнера. Если этот параметр единственный, то каждая из программ реализует функции стеганодетектора: производится сканирование контейнера с выводом результата на экран. Если таких параметров два, то стеганограмма извлекается из контейнера и расшифровывается. Результат

выводится в файл, указанный вторым параметром, а также на экран. При трех параметрах стега извлекается из файла, указанного вторым параметром, шифруется исключающим «ИЛИ» и помещается в файл контейнера, заданного первым. Модифицированной стеганограммой контейнер записывается в файл, заданный третьим параметром.

Для шифрования во всех случаях используется программный датчик случайных чисел, начальное состояние которого определяется константами Key1 и Key2. Всегда производится эхо-печать стега.

Для наглядности все программы написаны на входном языке компактного компилятора Turbo Pascal 3.x компании Borland.

Эффективность описанных методов упаковки стега в контейнере была исследована на переведенном в ASCII-вид тексте главы VI тома I книги «Мертвая вода» объемом 126 729 байт и насчитывающим 2143 строки со строками, выровненными на 65-символьную границу при абзацном отступе в четыре символа. Полученная плотность упаковки (в порядке возрастания) представлена в следующей таблице:

Сравнение методов текстовой стеганографии

Метод	Знаков стего	Плотность, %
Чередование маркеров конца	267	0,21
Выравнивание пробелами	411	0,32
Двоичные нули	740	0,58
Хвостовые пробелы	1071	0,85
Знаки одинакового начертания	4065	3,21

Обращает на себя внимание необычно высокая эффективность упаковки стега с использованием подмены символов.

Полученные данные являются лишь оценочными и зависят не только от свойств контейнера, но и от свойств помещаемого в него стега, хотя и в меньшей степени.

Число автоматических методов текстовой стеганографии, естественно, не ограничивается рассмотренными примерами. Пополнить запас примеров можно, в частности, разумной комбинацией уже приведенных.

В завершение стоит упомянуть об одном неожиданном наблюдении, свидетельствующем о том, что текстовых файлов, пригодных для использования в качестве стеганоконтейнера, намного больше, чем это может показаться с первого взгляда. Действительно, таковыми являются и файлы баз данных, символьные поля записей которых фактически представляют собой строки фиксированной длины (естественно, без завершающих символов CR/LF).

К недостаткам представленных методов следует отнести высокую вероятность разрушения скрытого сообщения при повторном наборе текста или

использовании более сложных текстовых редакторов, способных осуществлять ряд автоматических операций над текстом. Такие операции, как форматирование, замена символов табуляции пробелами, удаление лишних пробелов в конце строк и т.д., приведут к порче или же полному уничтожению скрытого сообщения. Значительно большей стойкостью к подобным искажениям обладают методы, оперирующие непосредственно самим текстом, отдельными его предложениями и словами.

Лингвистическая стеганография (***лексические или семантические методы),*** предполагает использование семантических особенностей языка. Данный подход отличается высокой эффективностью, обусловленной применением различных методов манипулирования не второстепенными элементами и незначительными особенностями текстов, а непосредственно самими предложениями и словами. Ряд методов, относящихся к данному направлению, основан на использовании синонимов. Практически в любом достаточно длинном предложении встречаются слова, которые без потери смысла могут быть заменены синонимами. Если для некоторого слова существует набор более чем из одного синонима, то возможно формирование специальных таблиц замен. В таких таблицах каждому синониму может быть поставлено в соответствие некоторое кодовое слово, состоящее более чем из одного двоичного символа. Однако необходимо отметить, что в ряде случаев использование методов осложнено определенными нюансами и оттенками ключевых слов в предложениях, что несколько ограничивает их применение.

Рассматривая работы зарубежных специалистов, посвященные лингвистической стеганографии, как например [120], можно заметить, что авторы этих работ достаточно четко разграничивают методы и алгоритмы лингвистической стеганографии по защите скрываемой информации от «роботов» (программ автоматического сканирования и анализа текстов) и от людей. Первые направлены на защиту информации при тотальном сканировании всей корреспонденции программными поисковыми роботами. Вторые направлены на защиту информации при внимательном просмотре текста человеком. Не вызывает удивления тот факт, что публикаций и работ, посвященных первому направлению на порядок больше работ, посвященных второму направлению (защите от анализа человеком). Поисковые роботы ищут ключевые слова, фразы, какие-то явные особенности текста. В результате, робота, который не силен в грамматике и не понимает смысла и явного подтекста передаваемых сообщений, обмануть гораздо проще. Задача же скрытой передачи информации в тексте, нацеленная на защиту от анализа передаваемого сообщения человеком, очевидно на порядок сложнее. Поэтому необходимо разработать и реализовать методы скрытой передачи коротких сообщений, использующие в качестве контейнеров текстовые файлы и при этом обеспечить защиту как от визуального анализа, проводимого человеком, так и от статистического анализа, который может быть проведен роботами.

Решить поставленную задачу для текстов, например, на русском (а тем более на украинском) языке в действительности значительно сложнее, нежели для текстов на английском языке. Здесь можно выделить два основных фактора, приводящих к усложнению задачи. Первым из них является неоднозначное использование слов в русском языке. В различном контексте одни и те же слова могут нести различную смысловую нагрузку. Вторым фактором является широкое использование в русском языке большого количества окончаний слов. Если при построении стеганографической системы не учитывать хотя бы один из этих факторов, результирующий текст будет носить явно несогласованный характер, что является очевидным демаскирующим признаком. В качестве основы для разработки новых методов был взят метод лингвистической стеганографии, основанный на использовании синонимов (метод замены синонимов). Принцип работы базового метода прост. Довольно часто в тексте одно слово может быть заменено другим словом, которое является синонимом исходного слова. В качестве примера можно привести два предложения, несущих одинаковую смысловую нагрузку: «На улице сейчас прекрасная погода» и «На улице сейчас замечательная погода». Так как предложения несут одинаковую смысловую нагрузку, то использование их в тексте эквивалентно. Для того чтобы передать скрытое сообщение первому предложению, мы можем поставить в соответствие двоичный «0», второму – двоичную «1» скрываемого сообщения. Как видно из представленного примера, использование стеганографического метода, основанного на замене синонимов, позволяет сохранить синтаксическую структуру предложения и его смысловую нагрузку. Такую замену слов достаточно легко проделать человеку. В то же время этот метод нельзя реализовать простым машинным алгоритмом, даже если не учитывать необходимость подстановки окончаний и согласования слов. Можно заметить, что в русском языке существует достаточно большое количество пар {слово; синоним}. Использование всех таких пар для целей стеганографического сокрытия информации, когда слову ставится в соответствие двоичный «0», а его синониму «1» очередного бита скрываемого сообщения, часто приводит к значительным искажениям смысловой нагрузки скрывающего текста. Как следствие, из-за неправильного употребления синонимов текст, содержащий скрытую информацию, становится легко идентифицируемым, и, в свою очередь, позволяет противнику установить наличие скрытого сообщения. Здесь появляется противоречие. Требование максимизации пропускной способности для метода скрытой передачи информации на основе замены синонимов, на первый взгляд, явным образом требует использования максимально большого словаря синонимов. Очевидно, что чем больше слов в используемом словаре синонимов, тем большее количество слов в тексте можно будет заменить и использовать для записи информации. Но чем больше слов в словаре синонимов, тем выше вероятность их неправильного употребления. Например, два слова «машина» и

«автомобиль» являются синонимами, но в предложении «Новая стиральная машина» синоним «автомобиль» использовать нельзя. Причина невозможности замены слова синонимом в приведенном выше примере объясняется тем, что мы столкнулись с неоднозначными синонимами, использовать которые можно только в зависимости от контекста. В действительности в русском языке можно выделить два класса синонимов: однозначные и неоднозначные. Первые могут быть использованы в любом контексте, вторые только в определенном смысловом значении. На первый взгляд лучшим решением было бы отказаться от использования неоднозначных синонимов и использовать для целей скрытой передачи информации только однозначные синонимы. Но такое решение приведет к сильному снижению информационной емкости контейнеров, так как однозначные синонимы составляют малую часть множества всех возможных синонимов. Компромисс все же может быть найден. Здесь следует отметить тот факт, что довольно большую группу синонимов составляют синонимы, употребление которых в несвойственном им контексте маловероятно. Включение таких синонимов в словарь позволяет значительно увеличить информационную емкость при относительно небольшом проценте неверных замен. В целях сведения к минимуму числа неконтролируемых замен синонимов вместо полного словаря синонимов для русского языка, можно использовать ограниченный словарь, состоящий только из наиболее часто употребляемых слов.

Однако словарь синонимов для стеганографического метода синонимичных преобразований может быть существенно ограничен без серьезной потери в информационной емкости. Если ограничить словарь синонимов только наиболее часто употребляемыми словами, то его будет гораздо легче грамотно обработать. В данном случае небольшая потеря в информационной емкости метода позволяет значительно улучшить его скрытность, которая непосредственно связана с качеством используемого словаря синонимов. Уменьшая размер словаря, мы тем самым предоставляем возможность для его внимательной проработки, которая, в свою очередь, позволит исключить использование редко употребляемых слов в несвойственном им контексте. В результате можно значительно снизить вероятность замены исходных слов в тексте синонимами с неподходящим для данного контекста значением.

Важно отметить, что применение простого метода замены слов можно считать приемлемым только в случае использования коротких текстовых сообщений. Использование данного метода для относительно больших текстов приведет к возможности обнаружения скрытого канала методами статистического анализа. Так если скрываемые данные будут представлять собой двоичные последовательности с равномерным распределением, то на выходе частоты слов могут сильно измениться. Редко употребляемые в обычных текстах слова будут использоваться наравне с наиболее часто употребляемыми словами. Для сохранения частотных характеристик текстов предлагается дополнить словарь

синонимов дополнительной таблицей частот встречаемости слов, входящих в словарь синонимов.

Так как для сокрытия информации используются только слова, входящие в словарь синонимов, то предложенная схема позволяет обеспечить возможность предварительного анализа объема контейнера без учета скрываемой информации. За счет этого можно подобрать скрывающий текст из множества предварительно подготовленных документов под конкретное скрываемое сообщение. Это, в свою очередь, позволяет избежать использования контейнеров большой емкости для передачи коротких сообщений и гарантировать возможность записи в контейнер заранее определенного объема скрываемой информации. Таким образом, можно рационально использовать заранее подготовленный набор текстовых документов и обеспечить работу всей системы в автоматическом режиме.

В русском языке слова довольно редко употребляются без соответствующих окончаний, позволяющих согласовать данное слово с его окружением в тексте. Данный факт необходимо учитывать при формировании словаря синонимов. Ведь практически любая замена слова, произведенная без учета его окончания, может привести к разрушению структуры предложения, что легко обнаружить. Следовательно, алгоритм сокрытия информации, работающий с русскоязычными текстами, при замене одних слов другими, непременно должен учитывать окончания этих слов. Здесь нужно особо отметить, что простая подстановка окончания исходного слова к заменяющему его слову не приведет к желаемому результату, так как даже существительные в одном и том же падеже могут иметь разные окончания. Кроме того, различные части речи используют различные механизмы словообразования.

Для решения этой проблемы предлагается разбить словарь синонимов на отдельные таблицы в соответствии с частями речи: существительные, прилагательные, числительные, местоимения, глаголы, наречия, предлоги, союзы, частицы и связки. Помимо самих слов, в таблицы заносятся и все возможные окончания в соответствии с падежом, родом, числом, склонением и спряжением. Эти окончания выписываются последовательно для каждого слова в отдельности. Если окончание отсутствует, то соответствующее поле остается пустым, но список через запятую продолжается дальше. В результате для каждого слова из словаря синонимов в первом приближении формируется список, состоящий из слов и всех возможных окончаний.

Простой алгоритм сокрытия информации в текстовых данных выглядит следующим образом. В простом варианте реализации алгоритма замена слов осуществляется без учета статистических данных. Он основан на простом методе замены слов. В этом случае вектор синонимов для каждого слова из словаря синонимов нормируется по длине, которая должна быть кратной степени двойки. В случае если длина вектора синонимов оказывается больше необходимой, то из него удаляются наиболее редко используемые синонимы. Количество битов скрываемой информации t для каждого слова определяется исходя из длины I

вектора синонимов: t = log21. Каждому из синонимов в векторе ставится в соответствие двоичное представление числа из диапазона 0, ..., 2t – 1. В процессе записи информации из очередного вектора синонимов выбирается слово, двоичное представление номера которого соответствует текущему двоичному вектору скрываемой информации длины t. Выбранное слово и становится заменой текущего слова. После того, как очередное замещающее слово было выбрано, оно вставляется в текст на место исходного слова с использованием соответствующего окончания.

Методы внедрения, основанные на семантических особенностях текста, являются трудно обнаружимыми. Замена одного слова на соответствующий ему синоним не нарушает синтаксическую структуру предложения и не искажает смысловое содержание. Несмотря на указанную особенность, такой метод внедрения также не лишен недостатков. При замене некоторых слов возможно нарушение стиля языка. Например, во фразе «what time is it?» слово time может быть заменено на синоним duration, но это будет некорректно для английского языка. Также использование некоторых слов в качестве синонимов может нарушать авторский стиль написания текста. На этих фактах базируются многие методы анализа. К недостаткам словарей синонимов первого приближения можно отнести тот факт, что в случае отсутствия окончания у исходного слова более чем в одной позиции или наличия двух и более одинаковых окончаний, становится невозможным точно подобрать окончание для замещающего его слова. Выбрать нужное окончание можно, если посмотреть в каком контексте употребляется исходное слово. Однако данную операцию не так легко реализовать программно.

Мимикрия. Методы использования имитирующих функций (mimic-function). Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение.

Для получения стегатекста используются контекстно-свободные грамматики. Нетерминальные символы могут быть раскрыты по заданным правилам несколькими возможными способами. В зависимости от входного сообщения выбирается правило раскрытия. Сгенерированный стегатекст не содержит грамматических и орфографических ошибок. На сегодняшний день самыми популярными программами, генерирующими искусственный текст, являются Nicetext, Texto и Markov-Chain-Based. Эти программы имеют высокое соотношение размера входного сообщения к размеру генерируемого текста, и получающийся текст максимально похож на естественный. Стоит отметить, что получившийся искусственный текст, как правило, является бессмысленным.

Устойчивость методов, генерирующих стегатекст, подобный естественному, обеспечивается заданными правилами грамматики. Отсутствие грамматических и орфографических ошибок в предложениях делает затруднительным поиск отличий искусственного текста от естественного. Анализ осмысленности текста можно производить только с участием человека, что не всегда возможно из-за огромного объема анализируемой информации. Наиболее эффективный метод

анализа использует прогнозирование для выявления искусственной природы текста, порожденного программой Nicetext. Сначала производится анализ слов первой половины текста, и составляется прогноз каждого последующего слова из второй части текста. Если в подавляющем большинстве случаев прогноз оказывается успешным, то это означает, что мы имеем дело с естественным текстом. Частые ошибки при прогнозировании могут свидетельствовать о наличии искусственного текста. Для программ Texto и Markov-Chain-Based используются методы, учитывающие корреляцию слов между предложениями. Так, считается, что предложения, содержащие слова, встречающиеся только в технических текстах, не могут стоять рядом с предложениями, содержащими слова, встречающиеся только в текстах художественной литературы.

Достоинством метода является то, что результирующий текст не является подозрительным для систем мониторинга. К недостаткам можно отнести слабую производительность метода, передачу небольших объемов информации и низкую степень скрытности в сети.

Стегоанализ. Существует также обратная стеганографии задача – стегоанализ. Задача стегоанализа состоит в обнаружении факта передачи секретного сообщения. Можно сказать, что стеганография и стегоанализ – два параллельно развивающихся направления науки. Так, для существующего метода стеганографии может быть разработан метод стегоанализа, который, как правило, накладывает ограничения на исходную схему встраивания информации в контейнер. Например, уменьшается допустимый объем передаваемой информации.

Стегоанализ получил широкое применение в сфере обеспечения информационной безопасности и, в частности, для борьбы с незаконной передачей информации. Например, в некоторых отечественных и иностранных компаниях служба безопасности проверяет исходящую электронную почту сотрудников для пресечения утечки закрытой коммерческой информации. Принимая во внимание широкую доступность и разнообразие программных продуктов, позволяющих встраивать скрытую информацию в обычные «невинные» письма, становится очевидной актуальность совершенствования методов стегоанализа. Учитывая большой объем передаваемых данных, перспективными следует считать методы компьютерного анализа, работающие без участия человека.

Стегоанализ также может быть применен злоумышленником. Например, для случаев с цифровыми отпечатками пальцев в программе, атакующий может выявить факт существования специальных меток в программе и попытаться их исказить или удалить. В таком случае развитие методов стегоанализа необходимо для установления потенциальных возможностей злоумышленника и, соответственно, для корректировки схем внедрения скрытой информации.

Следует отметить, что защиты требует только изображение информации, представленное на материальном носителе, причем под ней понимается создание условий, исключающих либо затрудняющих доступ к носителю, внесение изменений или уничтожение носителя, а также восприятие представленных на

нем данных, производимое с помощью методов криптографии и стеганографии. И если, образно говоря, криптография делает понятное непонятным, то стеганография делает видимое невидимым (иногда и в прямом смысле слова). Достигается это «растворением» скрываемой информации среди других данных значительно большего объема.

Что касается стегоанализа сообщений при использовании методов текстовой стеганографии, интересным является метод стегоанализа, основанный на подходе Рябко Б.Я. [120], который заключается в том, что для выявления факта наличия стеготекста используется сжатие обычным архиватором. Основная идея подхода состоит в том, что внедряемое сообщение нарушает статистическую структуру контейнера, повышая его энтропию. Следовательно, заполненный контейнер будет «сжиматься» хуже, чем незаполненный. В отличие от предыдущих известных аналогов, данный метод обладает рядом преимуществ:

- метод имеет самую высокую точность из ранее известных аналогов;
- анализ занимает сравнительно мало времени (порядка 0,1 – 0,5 с. на современных персональных компьютерах);
- необходим меньший объем входных данных по сравнению с другими методами;
- для проведения анализа не требуется словарей синонимов или правил грамматики языка, занимающих большой объем памяти.

Заключение. Итак, были рассмотрены различные методы обеспечения безопасности использования информационных технологий за счет встраивания скрытой информации в тестовые файлы, каждый из которых имеет свои преимущества и недостатки. На основе предложенного анализа каждый отдельный пользователь может сделать самостоятельный обоснованный выбор приемлемого метода в зависимости от круга решаемых задач. Предложенные алгоритмы, базирующиеся на методах цифровой стеганографии, могут быть использованы, например, для построения систем защиты авторских прав собственников и пользователей текстовой информации, представленной в цифровой форме, а также для анализа и фильтрации передаваемого трафика в сети с целью пресечения утечки коммерческой информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Amerini I. Copy-move forgery detection and localization by means of robust clustering with J-linkage / I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, L. del Tongo, G. Serra // Signal Processing. – 2013. – T.28. – №6. – C. 659–669.
2. Bennett K. Linguistic Steganography: survey, analysis, and robustness concerns for hiding information in text, Center for Education and Research in Information Assurance and Security, CERIAS Tech Report 2004 – 13. – 30 pp.
3. Bhattacharya J. Rudiments of computer science. Kolkata.2010.
4. Bohm C. Flow Diagrams, Turing Machines and Languages with Only Two Formation Rules. / C. Bohm, G. Jacopini – Comm. Of the ACM, V.9. – 1966. – PP. 366 – 371.
5. Brent Richard and Zimmermann Paul. Modern Computer Arithmetic // Cambridge Monographs on Computational and Applied Mathematics (No. 18), Cambridge University Press, November 2010. – 239 p.
6. Brumnik R. Techniques For Performance Increasing Of Integer Multiplications In Cryptographic Application. / R. Brumnik, V. Kovtun, A. Okhrimenko, S. Kavun – Mathematical Problems in Engineering. – vol. 2014. – 2014. – p. 7.
7. Dupaquis V. Redundant Modular Reduction Algorithms. Smart Card Research and Advanced Applications. Lecture Notes in Computer Science / V. Dupaquis, A. Venelli – Volume 7079. – 2011. – PP. 102 – 114.
8. Evaluation of hypothetical attacks against PassWindow [Electronic resource] / Sean O'Neil // PassWindow – 2009. – Access mode: http://www.passwindow.com/ evaluation_of_hypothetical_attacks_against_passwindow.
9. Farid H. Image Forgery Detection / H. Farid // IEEE Signal processing magazine. – 2009. – P. 16 – 25.
10. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.
11. Getman A. A crowdsourcing approach to building a legal ontology from text / A. P. Getman, V. V. Karasiuk // Artificial Intelligence and Law. – 2014. Vol. 22, Num. 3, – P. 313 – 335.
12. Herega A. Dynamical chaos in four dimension phase space: Introduction to classification / A. Herega, I. Kononovich, V. Rats // Computer Technologies in Physical and Engineering Applications (ICCTPEA) International Conference on. – St. Petersburg IEEE, 2014 (DOI 10.1109/ICCTPEA.2014.6893276). – Regime access: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6893276&url= http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F6881321%2F6893238%2F06893276.pdf%3Farnumber%3D6893276.
13. Kononenko Igor V. Computerizing of Production and Economic Systems Development Management. /I. V. Kononenko. – Black & White, 2012. – 334 p.

14. Kostiuk A. A new recurrence data encode method in information systems of management / A. Kostiuk, L. Petryshyn // W: Zarządzanie przedsiębiorstwem – teoria i praktyka: XIV międzynarodowa konferencja naukowa : 22–23 listopada 2012, Kraków : materiały konferencyjne. / Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie. — Kraków : WZ AGH, cop. 2012. – P. 1 – 5.

15. Lhote L., Vallée B Sharp Estimates for the Main Parameters of the Euclid Algorithm. LATIN 2006: Theoretical Informatics. Lecture Notes in Computer Science Volume 3887, 2006. – PP. 689 – 702.

16. Marketing channel [Electronic resource]. – Mode of access : http//en.wikipedia.org/ wiki / Marketing_channel.

17. NESSIE consortium "NESSIE Security report." Deliverable report D20 – NESSIE, 2002. – NES/DOC/ENS/WP5/D20 [Electronic resource]. – Access mode: http://www.cryptonessie.org/.

18. Olijnykov R. An Impact of S-box Boolean Function Properties to Strength of Modern Symmetric Block Ciphers / R. Olijnykov, O. Kazymyrov // Радиотехника, 2011. Вып. 116. – С. 11 – 17.

19. Preparata Franco P. On the Representation of Integers in Nonadjacent Form // SIAM Journal on Applied Mathematics. – Vol. 21. -No. 4. -1971. – PP. 630 – 635.

20. Rey C. A survey of watermarking algorithms for image authentication / C. Rey, J.-L. Dugelay // EURASIP J. Appl. Signal Process. – 2002. – №1. – С. 613 – 621.

21. Smirnov A.A. Experimental studies of the statistical properties of network traffic based on the BDS-statistics / A.A. Smirnov, D.A. Danilenko // International Journal of Computational Engineering Research (IJCER). – Volume 4, Issue 5. – India. Delhi. – 2014. – P. 41 – 51.

22. Stehle D., Zimmermann P. A Binary Recursive Gcd Algorithm. Algorithmic Number Theory. Lecture Notes in Computer Science Volume 3076, 2004. – PP. 411 – 425.

23. WEB-application [Электронный ресурс] // Сайт информатики и программирования для студентов и школьников. – Режим доступа: http://inflib.ru/slovar-spravochnik-po-terminam/setevyie-tehnologii/web-prilozheniya-veb-prilozheniya-web-application.html. – Название с экрана.

24. Абросимов А.Г. Информационно-образовательная среда ВУЗа [Электронный ресурс] / А.Г. Абросимов. — Электрон. дан. — Режим доступа: http://comparative.edu.ru:9080/PortalWeb/data/00004047/2.pdf.

25. Автоматический анализ сложных изображений [Сборник переводов] / Под ред. Э.М. Бравермана – М.: Издательство Мир, 1969. – 308 с.

26. Айвазян С. А. Прикладная статистика: Классификация и снижение размерности [Текст] / С. А. Айвазян, В. М. Бухштабер, И. С. Енюков и др. – М.: Финансы и статистика, 1989. – 607с.

27. Алешин Г.В., Урвачев В.И. Оптимизация подвижных линий связи со

сверхузкими диаграммами направленности излучателей. В кн. «Некоторые вопросы повышения эффективности и помехоустойчивости радиоэлектронных систем». – Х.: ХВВУ, 1973, Вып. 331.

28. Алешин Г.В. Эффективность сложных радиотехнических систем. / Г.В. Алешин , Ю.А. Богданов – К.: «Наукова думка», 2008. – 288 с.

29. Альошин Г.В. Оцінка якості інформаційно-вимірювальних систем. / Г.В. Алешин – Х.: УкрДАЗТ, 2008. – 300 с.

30. Ансофф И. Новая корпоративная стратегия. / И. Ансофф. – СПб.: Издательство «Питер», 1999. – 416 с.

31. АСУ городским хозяйством / И.В. Кузьмин, Э.Г. Петров, И.А. Алферов, В.В. Евсеев, Л.В. Мигунова. – Киев, − «Будівельник», 1978. – 144 с.

32. Баркалов С. А. Модели и механизмы в управлении организационными системами / С. А. Баркалов, В. Н. Бурков, Д. А. Новиков, Н. А. Шульженко – М.: Тульский полиграфист, 2003. – Т. 1. – 560 с., Т. 2. – 380 с., Т. 3. – 205 с.

33. Белецкий А. Я. Обобщенные коды Грея. / А. Я. Белецкий. – «Palmarium Academic Publishing», Germany, 2014. – 208с.

34. Беляев А. Стеганограмма: скрытие информации // Программист, 2002, №1. [Электронный ресурс]. Режим доступа: www.alinkamalinka7.narod.ru/referist.doc.В. Текин. Текстовая стеганография // Мир ПК. – 2004. – № 11. – С. 6263

35. Библиотека многократной точности GMP. [Электронный ресурс]. Режим доступа : https://gmplib.org

36. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М. : Мир, 1986. – 576 с.

37. Браткевич В. В. Количественная оценка качества мультимедийной продукции. / В. В. Браткевич, А.И. Пушкарь // Информационные системы в управлении, образовании, промышленности: монография / под ред. В.С. Пономаренко. –Х. Вид-во ТОВ «Щедра садиба плюс». – 2014. – 498 с.

38. Браткевич В. В. Оптимизация связей между критериями оценки качества мультимедийных изданий / В.В. Браткевич / Системи обробки інформації // Проблеми і перспективи розвитку ІТ-індустрії. – Випуск 7 (97). – Х. : 2011. – С. 84.

39. Бурков В. Н. Как управлять организациями / В. Н Бурков, Д. А. Новиков. – М. : СИНТЕГ. – 2004. – 400 с.

40. Бутман Е. Эволюция каналов сбыта [Электронный ресурс] // Бизнес-журнал. – 2012. – № 5. – Режим доступа : http://www.marketing.spb.ru/lib-mm/sales/channel_evol.htm?printversion.

41. Ватолин Д. Методы сжатия данных / Д.Ватолин, А.Ратушняк, М.Смирнов, В.Юкин. – ДИАЛОГ-МИФИ, 2003. – 381 с.

42. Воронин А. А. Оптимальные иерархические структуры / А. А. Воронин, С. П. Мишин. – М. : ИПУ РАН – 2003. – 214 с.

43. Гантмахер Ф.Р. Теория матриц / Ф.Р.Гантмахер. – М.: Наука, 1988. – 552 с.

44. Годлевский М.Д. Принципы управления функционированием и развитием холдинга на основе ключевых показателей эффективности / Э.Е. Рубин, С.С. Никитчук – Вестник НТУ «ХПИ». – С. 46 – 54.

45. Граничин О. Н. Рандомизированные алгоритмы в задачах обработки данных и принятия решений. / О. Н. Гаранин // Системное программирование. Вып. 6, 2012. – С. 141 – 162. – Режим доступа: http://www.math.spbu.ru/user/gran/papers/10580575.pdf.

46. Грибунин В.Г. Цифровая стеганография [Текст]: монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

47. Григорьев С.Г. Основные принципы и методики использования системы порталов в учебном процессе / С.Г. Григорьев, В.В. Гриншкун, Г.А. Краснова // Интернет-порталы: содержание и технологии. – № 2. – М.: Просвещение, 2013. — С. 56 – 84.

48. Двухфакторная Аутентификация [Электронный ресурс] // Aladdin – 2014. – Режим доступа: http://www.aladdin-rd.ru/solutions/authentication.

49. Динамический хаос. – Режим доступа: https://www.google.ru/?gws_rd=ssl#newwindow=

50. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР. Остання редакція від 02.03.2014. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

51. Засядько А.А. Дифференциально-тейлоровская модель задачи восстановления в спектроскопии / А.А. Засядько // Электронное моделирование. – 2002. – Т.24. – № 6. – С. 97 – 105.

52. Засядько А.А. Моделювання процесу відновлення сигналів методом диференційно-тейлорівських перетворень / А.А. Засядько // Вісник ЖІТІ. – 2001. – № 18 / Технічні науки. – С. 101 – 104.

53. Зензин О. С. Стандарт криптографической защиты – AES. Конечные поля. / О. С. Зензин, М. А. Иванов. Под ред. М. А. Иванова. – М.: КУДИЦ-ОБРАЗ. – 2002. – 176 с.

54. Иванов В. Г. Сжатие изображения текста на основе статистического анализа и классификации вертикальных элементов строки [Текст] / В. Г. Иванов, Ю. В. Ломоносов, М. Г. Любарский // Восточно-Европейский журнал передовых технологий. - Харьков. – 2014.- № 4/2 (70). – с. 4 – 15.

55. Иванов В. Г. Сжатие изображения текста на основе выделения символов и их классификации [Текст] / В. Г. Иванов, М. Г. Любарский, Ю. В. Ломоносов // Проблемы управления и информатики. – 2010. – № 6. – С. 111 – 122.

56. Иванов В. Г. Сжатие изображения текста на основе формирования и классификации вертикальных элементов строки в графическом словаре

символьных данных [Текст] / В. Г. Иванов, М. Г. Любарский, Ю. В. Ломоносов // Проблемы управления и информатики. – 2011. – № 5. – С. 98 – 109.

57. Иванов В.Г. Сжатие изображения текста на основе формирования и классификации вертикальных элементов строки в графическом словаре символьных данных / В.Г. Иванов, М.Г. Любарский, Ю.В. Ломоносов // Проблемы управления и информатики. – К. – 2011. – № 5. – С. 98 – 109.

58. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

59. Иванов С. Н. Использование онтологической модели учебных ресурсов в правоведении / С.Н. Иванов, В.В Карасюк // Инновации и современные технологии в системе образования : материалы III международной научно-практической конференции 20–21 февраля 2013 года. – Прага : Vědecko vydavatelské centrum «Sociosféra-CZ», 2013. – С. 174 – 177.

60. Иванов В.Г. Сжатие изображения текста на основе выделения символов и их классификации. / В.Г. Иванов , Ю.В. Ломоносов , М.Г. Любарский – Киев: Международный научно-технический журнал «Проблемы управления и информатики». – 2010, №6. – С. 111 – 122.

61. Ивлев А.А. Основы теории Джона Бойда. Принципы, применение и реализация / А.А. Ивлев. 2009 – Режим доступа: http://www.milresource.ru/Boyd.html.

62. Информационные системы в управлении, образовании, промышленности. [Коллективная монография]. [Алешин Г.В., Коломийцев А.В. и др.]; под ред. В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014, – 498 с.

63. Іванов С. М. Створення індивідуального інформаційного простору для навчання студента правника / С. М. Іванов, В. В. Карасюк, С. В. Глинянський // Інноваційні комп'ютерні технології у вищій школі (ІСТ-2014): Праці VI Науково-практичної конференції (18-20 листопада 2014, Львів). – Львів, Національний університет «Львівська політехніка» – С. 150 – 155.

64. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.

65. Казакова Н.Ф. Моніторинг інформаційних ресурсів в захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Світ інформації та телекомунікацій : VII міжнар. наук.-техн. конф. студентства та молоді, 15-16 квітня 2010 р. – ДУІКТ, Київ. – С. 165-168.

66. Казакова, Н. Ф. Некоректні задачі відновлення даних у системах моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 8(179). – Т. 1. – С. 325 – 332.

67. Казакова, Н. Ф. Оцінка живучості систем моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. – Харьков : Технологический центр. – 2012 – № 4/2(58). – С. 12 – 15.

68. Казакова, Н. Ф. Питання теорії детермінованої регуляризації некоректних задач відновлення інформації в системах моніторингу спеціального призначення [Текст] / Н. Ф. Казакова, А. О. Петров // Інформаційно-вимірювальні технології в метрології, технічне регулювання та менеджмент якості : III всеукр. наук.-практ. конф., 30-31 травня 2013 р. : матер. конф. – Одеса : ОДАТРЯ. – С. 81 – 83.

69. Казимиров А. В. Метод построения нелинейных узлов замены на основе градиентного спуска. / А. В. Казимиров, Р. В. Олейников // Радиотехника: Всеукр. межвед. научно техн. сб. – 2013. – Вып. 172: Информ. безопасность. – С. 104 – 108.

70. Камер Дуглас Э. Сети TCP/IP, том 1. Принципы, протоколы и структура / Камер Дуглас Э. – М.: Издательский дом "Вильямс", 2003. – 445с.

71. Карасюк В.В. Дистанционные методы изучения гуманитарных дисциплин / В.В. Карасюк, Н.А. Кошевая, Н.И. Мазниченко // Инновационные информационные технологии: Материалы международной научно-практической конференции. Том 1. / Гл. ред. С.У. Увайсов – М.:МИЭМ НИУ ВШЭ, 2013. – С. 222 – 229.

72. Карасюк В.В. Формирование индивидуального образовательного пространства студента в условиях дистанционного обучения / В.В. Карасюк, С. Н. Иванов // Вестник Национального технического университета «Харьковский политехнический институт». Сборник научных трудов. Серия: Информатика и моделирование. – Харьков: НТУ «ХПИ». – 2014. – № 35 (1078). – С. 105 – 112.

73. Клачек П. М.Технологическая платформа как инструмент регионального инновационного развития экономики России. / П. М. Клачек, С. И. Корягин, Е.С. Минкова // Научно-технические ведомости СПбГПУ № 4, серия «Экономические науки». – СПб.: Изд-во Политехн. ун-та, 2011. – С. 35 – 39.

74. Клейнер Г. Б. Предприятие в нестабильной экономической среде: риски, стратегии, безопасность / Г. Б. Клейнер, В. А. Тамбовцев, Р. М. Качалов. – М.: Экономика, 1997. – 288 с.

75. Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. – К.: Изд.ГУИКТ, 2009. – 251 с.

76. Кобозева А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2012. – Вип. 38. – С. 193–203.

77. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / Коваленко А.С., Смірнов О.А., Коваленко О.В // Системи озброєння і військова техніка. – Випуск 1(37) – Х.: ХУПС – 2014. – С. 86 – 90.

78. Ковбасюк С.В. Методика определения параметров нелинейных систем на основе дифференциально–нетейлоровских преобразований / С.В. Ковбасюк, А.А. Писарчук //Двойные технологии. – 2004. – № 1. – С. 30 – 34.

79. Комп'ютеризовані системи і технології видавничо-поліграфічних виробництв: монографія / Під ред. О. І. Пушкаря. – Харків: ІНЖЕК, 2011. – 296 с. (подраздел 4.1. Методика розробки поліграфічного калькулятора для розрахунку вартості замовлення).

80. Конахович Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. – 288 с.

81. Король О. Г. Исследование методов обеспечения аутентичности и целостности данных на основе односторонних хеш-функций / О. Г. Король, С. П. Евсеев. // Науково-технічний журнал «Захист інформації». Спецвипуск (40). – 2008. – С. 50 – 55.

82. Кристиан Венц. Программирование в ASP.NET AJAX / Кристиан Венц. – М.: Символ-Плюс. – 2008 – 510 с.

83. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) – Мн. : Харвест, 1999. – 363 с. – Режим доступа: http://www.evartist.narod.ru/text19/001.htm.

84. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 504 с.

85. Леоненков А.В. Самоучитель UML. – СПб.: БХВ-Петербург, 2001. – 304 с.

86. Лидл Р. Конечные поля. Монография в 2-х томах. / Р. Лидл, Г. Нидеррайтер. – Т. 1. – М.: Мир. – 1988. – 432 с.

87. Лосев Ю.И. Автоматизация в сетях с коммутацией пакетов / Ю.И. Лосев, М.Ю. Лосев, Ф.К. Яковец . – К: «Техніка» – 1994. – 212 с.

88. Макаров И. М. Теория выбора и принятие решений: Учебное пособие / И. М. Макаров, Т. М. Виноградская, А. А. Рубчинский, В. Б. Соколов. – М.: Наука. Главная редакция физико-математической литературы – 1982. – 328 с

89. Макгрегор Д. Тестирование объектно-ориентированного программного обеспечения. Практическое пособие. / Д. Макгрегор, Д. Сайкс. – К.: ООО "ТИД ДС" – 2002. – 432 с.

90. Межиров И. Курсовая работа на тему «Алгоритмы сжатия данных». – Москва, МГУ им. Ломоносова, механико-математический ф-т, научный руководитель А. Шень, 2004.

91. Мельник М.А. Методика сравнительной оценки устойчивости стеганографических алгоритмов к сжатию / М.А. Мельник // Сучасна спеціальна техніка. – 2013. – №4. – С. 67–74.

92. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – № 2(8). – С. 99 –106.

93. Мобільна радіолокаційна станція П-18. Будова, принцип дії систем та пристроїв. Навчальний посібник. – К.: ТОВ «Чайка-Всесвіт», 2006. – 162 с.

94. Мордвинов В. А. Полный менеджмент проектов информационных систем и порталов в образовании (разработка и внедрение в образовании наукоемкой методики проектирования ИС и порталов) / В.А. Мордвинов. — М.: Госинформобр, 2004. — 81 с.

95. Найк Д. Стандарты и протоколы Интернета / Найк Д. – М.: Символ, 2009. – 384 с.

96. Настройка двухфакторной аутентификации [Электронный ресурс] // Citrix – 2012. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.

97. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман., О. Моргенштерн / Пер. с англ. Н.Н. Воробьева. – М.: Наука, 1970. – 124 с.

98. Николас Закас. Ajax для профессионалов / Николас Закас, Джереми Мак-Пик, Джо Фосетт. – М.: Символ-Плюс, 2008. – 488 с.

99. Овезгельдыев А.О. Синтез и идентификация моделей многофакторного оценивания и оптимизации/ Овезгельдыев А.О., Петров Э.Г., Петров К.Э. – К: Наукова думка, 2002. –164с.

100. Оксеноид О. АСУ для оперативной полиграфии: взгляд изнутри // Publish. – 2004. – № 9. – С. 39–43.

101. Охрименко А.А. Арифметика с отложенным переносом. / А.А. Охрименко– Захист інформації. – 2014. – Т.16. – №2. – С. 130 – 138.

102. Пастухова В.Л. Визначення стратегічних альтер-натив розвитку підприємства на підставі кількісної оцін-ки впливу маркетингового середовища. / В.Л. Пастухова // Вісник КДТЕУ. – 1999. – №3. – С. 57 – 64.

103. Петришин Л.Б. К определению свойств унитарной системы счисления / Л.Б. Петришин, А.А. Борисенко // Электроника и системы управления. Науковий журнал. Национальный Аэрокосмический Университет. – Київ, 2008, Nr 3 (17) – С. 64 – 69.

104. Петришин Л.Б. Новий числовий ряд для визначення вагової мережі позиційної системи числення, альтернативної та алгоритмічно подібної системі Фібоначчі. // Матеріали 19-ї міжнародної конференції з автоматичного управління «Автоматика / Automatics – 2012». 26 – 28 вересня 2012, – Київ: Вид-во Національного університету харчових технологій. 2012. – С. 433 – 434.

105. Петришин Л.Б. Позиційна система числення, альтернативна системі Фібоначчі./ Л.Б. Петришин, А.Б. Костюк // Методи та засоби кодування, захисту й ущільнення інформації: четверта міжнар. наук.-практ. конф., 23-25.04.2013 р. – Вінниця: УНІВЕРСУМ-Вінниця, 2013. – С. 35 – 39.

106. Петришин Л.Б. Фибоначчи-подобный метод кодирования сообщений и полибоначчи способ перехода к двоичному исчислению. / Л.Б. Петришин // Вісник східноукраїнського національного університету імені В.Даля № 15 (204) Ч.1, Луганськ. 2013 – С. 158 – 165.

107. Петров Э. Г. Метод решения задачи распределения инвестиций в условиях многокритериальности с учетом интервальных неопределенностей исходных данных / Э. Г. Петров, Н. А. Брынза // Економіка розвитку . – 2014. – № 1. – С. 128 – 135.

108. Подиновский В.В. Парето-оптималные решения многокритериальных задач / В.В. Подиновский, В.Д. Ногин. – М.: Наука, 1982. – 254с.

109. Пономаренко В.С. Информационные технологии и системы в управлении, образовании, науке: Монография / В.С. Пономаренко, С.П. Євсеєв, М.Ю. Лосєв, С.В. Мінухін.– Х.: Цифрова друкарня №1, 2013. – 278с.

110. Пономаренко В.С. Методи та моделі розроблення комп'ютерних систем і мереж. Монографія / В.С. Пономаренко, С.П. Євсеєв, С.В. Кавун, М.Ю. Лосєв, С.В. Мінухін. – Харків: Вид. ХНЕУ, 2008. – 316 с.

111. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. – [Чинний від 2005-11-08]. – К.: ДСТСЗІ СБ України, 2005. – 16 с. – (Нормативний документ системи технічного захисту інформації).

112. Постанова Кабінету Міністрів України від 17 вересня 2008 р. N 834 «Про затвердження Державної цільової науково-технічної програми створення державної інтегрованої інформаційної системи забезпечення управління рухомими об'єктами (зв'язок, навігація, спостереження)».

113. Пратт В.К. Лазерные системы связи. – М.: Связь, 1972. – 232 с.

114. Прикладная статистика: Классификация и снижение размерности: [Справочник] / С.А. Айвазян, В.М. Бухштабер, И.С. Енюков и др.; Под ред. С.А. Айвазяна. – М.: Финансы и статистика, 1989. – 607с.

115. Пухов Г.Е. Дифференциальные преобразования функций и уравнений. / Г.Е. Пухов– К.: Наук. думка, 1980. – 419 с.

116. Пухов Г.Е. Приближенные методы математического моделирования, основанные на применении дифференциальных Т–преобразований. / Г.Е. Пухов – К.: Наук. думка, 1988. – 216 с.

117. Рамбо Дж., Джекобсон А., Буч Г. UML. Специальный справочник: Пер. с англ. – СПб.: Питер, 2002. – 656 с.

118. Распознавание радиолокационных целей по сигнальной информации. [Монография]. [Казаков Е.Л., Казаков А.Е. и. др.]; под ред. Е.Л. Казакова. – Х.: КП «Городская типография», 2010. – 232 с.

119. Российская полиграфия. Состояние, тенденции и перспективы развития. Отраслевой доклад. 2014 год. / Под. ред. В. В. Григорьева. – М.: Федеральное агентство по печати и массовым коммуникациям. – 2014. – 96 с.

120. Рябко Б.Я. Основы современной криптографии и стеганографии. / Б.Я. Рябко, А.Н. Фионов – М.: Горячая линия – Телеком, 2010. – 232 с.

121. Саати Т. Принятие решений при зависимостях и обратных связях. / Т. Саати. – Пер. С англ. – М.: «ЛКИ», 2008. – 360 с.

122. Саати Т. Принятие решений. Метод анализа иерархий. / Т. Саати. – Пер. Р. Г. Вачнадзе. – М.: «Радио и связь», 1993. – 278 с.

123. Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. – М.: Радио и связь, 1989. – 316 с.

124. Саркисян С.А. Большие технологические системы. Анализ и прогноз развития / С.А. Саркисян, В.М. Ахундов, Э.С. Минаев. – М.: Наука, 1977. – 350 с.

125. Семенов С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ «ХПІ», 2012. – Вип. 38. – С. 163-171.

126. Семь методов двухфакторной аутентификации [Электронный ресурс] // ITC.ua – 2007. – Режим доступа: http://www.infosecurityrussia.ru/news/29947.

127. Сеньківський В. М. Автоматизоване проектування книжкових видань: Монографія. / В. М. Сеньківський, Р. О. Козак. – Львів: Українська академія друкарства, 2008. – 200 с.

128. Система ASystemWeb [Электронный ресурс] // Сайт Арт-Point. – Режим доступа: http://www.art-point.com.ua/vozmozhnosti-programmy-asystemweb.html. – Название с экрана.

129. Скородумов П. В. Моделирование экономических систем с помощью аппарата сетей Петри [Электронный ресурс] П. В. Скородумов // Экономические и социальные перемены: факты, тенденции, прогноз. – 2014. – 4 (34). – Режим доступа : http://ssrn.com/abstract=2509029.

130. Скрыпникова М. Н. Великая информационная глобализация / М. Н. Скрыпникова // Российское предпринимательство. – 2002. – № 5 (29). – С. 95 – 98.

131. Смирнов А.А. Дисперсионный анализ сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 2(118). – Х.: ХУПС – 2014. – С. 124 – 133.

132. Смирнов А.А. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137 – 141.

133. Смирнов А.А. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Системи управління, навігації та зв’язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120 – 125.

134. Смірнов О.А. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова,

О.В. Коваленко // Системи обробки інформації. – Харків: ХУ ПС. – 2013 – Вип. 6(113). – С. 255 – 257.

135. Соколов Н. П. Пространственные матрицы и их приложения. / Н. П. Соколов. – М.:ГИФМЛ, 1960. – 300 с.

136. Сосулин Ю.Г.Теоретические основы радиолокации и радионавигации. - М. Радио и связь, 1992. – 304 с.

137. Стайкуца С.В. Оцінка інформаційної та фізичної безпеки системи аналітично-прогностичної інформації / С.В. Стайкуца // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький: – № 4 – 2014. – С. 220 – 225.

138. Стандартный глоссарий терминов, используемых в тестировании программного обеспечения. Версия 2. (от 4 декабря 2008). Подготовлен ‘Glossary Working Party’ International Software Testing Qualifications Board. 2008. – 55 с.

139. Статистичні дані. Видавнича справа // Державний комітет телебачення та радіомовлення України [Електрон. ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/category/main?cat_id=34099.

140. Стеганография, цифровые водяные знаки и стеганоанализ: Монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. М.: Вузовская книга, 2009. – 220 с.

141. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. / В. Столлингс : пер. с англ. – М.: издательский дом «Вильям», 2001. – 672 с.

142. Стюгин М. Оценка безопасности системы информационного управления Российской Федерации. – Режим доступа: http://psyfactor.org/lib/styugin4.htm.

143. Тихомиров В.П. Виртуальная образовательная среда: предпосылки, принципы, организация / В.П. Тихомиров, В.И. Солдаткин, С.Л. Лобачев // Международная академия открытого образования. — М. : Издательство МЭСИ, 2010. — 164 с.

144. Тихонов А.Н. Методы решения некорректных задач / А.Н. Тихонов, В.Я. Арсенин – М.: Наука, 1986. – 286 с.

145. Томпсон А.А. Стратегический менеджмент. Искусство разработки и реализации стратегии: Учебник для вузов. / А.А. Томпсон, А.Дж. Стрикленд. / Пер. с англ. под ред. .Г. Зайцева, М.И.Соколовой. – М.: Банки и биржи, ЮНИТИ, 1998. – 578 с.

146. Трухаев Р.И. Инфлюентный анализ и принятие решений / Р.И. Трухаев. – М.: Наука, 1984. – 235с.

147. Умножения целых чисел с использованием отложеного переноса для криптосистем с открытым ключом / В.Ю.Ковтун, А.А.Охрименко [и др.] // Информационные технологи и системы в управлении, образовании, науке: Монография / Под ред. проф. В.С. Пономаренко. – Х.: Цифрова друкарня №1. – 2013.– С. 69 – 82.

148. Ушакова І. О. Моделювання інформаційного впливу соціальних мереж на лояльність клієнтів / І. О. Ушакова // Сучасні методи та моделі обробки даних в інформаційних системах : монографія. – Харків: Вид. ХНЕУ, 2013. – 540 с.

149. Фаріон І.Д. Практикум з стратегічного аналізу. / І.Д. Фаріон, В.А. Чичун, С.М. Жукевич / За ред. Докт. Екон. Наук, проф. Фаріона І.Д. – Тернопіль, 2004. – 300 с.

150. Федонін О.С. Потенціал підприємства: формування та оцінка. / О.С. Федонін, І.М. Рєпіна, О.І. Олексюк. – К.: КНЕУ, 2003. – 316 с.

151. Филимонов А. Протоколы Интернета / Филимонов А. – СПб.: БХВ-Петербург, 2006. – 528 с.

152. Филимонов А.Ю. Протоколы Интернета. – СПб.: БХВ-Петербург, 2003. – 528с.

153. Фляйшер К. Стартегический и конкурентный анализ. Методы и средства конкурентного анализа в бизнесе. / К. Фляйшер, Б. Бенсуссан. – М.: БИНОМ, 2005. – 541 с.

154. Черненко, С. С. Применение мониторинга для обеспечения безопасности информационных систем [Електронний ресурс] / С. С. Черненко, А. С. Барабошин, Е. И. Лысенко, Л. С. Духнина // Портал : Современные проблемы науки и образования. – Режим доступу \www/ URL: http://www. science-education.ru/118-14171. – Заголовок з екрану, доступ вільний, 01.02.2015.

155. Шлезингер М. И. Математические средства обработки изображений [Текст] / М. И. Шлезингер. – Киев: Наукова думка, 1983. – 200 с.

156. Штерн Л. В. Маркетинговые каналы / Л. В. Штерн, А. И. Эль-Ансари, Э. Т. Кофлан ; [пер. с англ]. – М. : «Вильямс», 2002. – 624 с.

157. Штойер Р. Многокритериальная оптимизация. Теория, расчет и приложения / Р. Штойер. – М.: Радио и связь, 1992. – 504с.

НАУКОВЕ ВИДАННЯ

**Альошин Генадій Васильович, Белецький Анатолій Яковлевич,
Биккузин Кирило Валерійович, Бринза Наталля Олександрівна,
Бондар Ірина Олександрівна, Браткевич Вячеслав Вячеславович,
Вільхівська Ольга Володимирівна, Гвозденко Маріна Владиславівна,
Грабовський Євген Миколайович, Дудикевич Валерій Богданович,
Євсеєв Сергій Петрович, Засядько Аліна Анатоліївна,
Іванов Станіслав Миколайович, Іванов Володимир Георгійович,
Казакова Надія Феліксівна, Карасюк Володимир Васильович,
Кобозева Ала Анатоліївна, Коваленко Ганна Степанівна,
Коваленко Олександр Володимирович, Ковтун Владислав Юрійович,
Ковтун Марія Григорівна, Коломійцев Олексій Володимирович,
Кононович Володимир Григорович, Кононович Ірина Володимиріва,
Король Ольга Григорівна, Коц Григорій Павлович,
Кошева Наталля Анатоліївна, Ломоносов Юрій Вячеславович,
Лисенко Ірина Анатоліївна, Любарський Михайло Григорович,
Лосєв Михайло Юрійович, Мазніченко Наталля Іванівна,
Максимович Володимир Миколайович, Манєва Росиця Ілянівна,
Мельнік Маргарита Олександрівна, Микитин Галіна ВАсилівна,
Мохамад Абу Таам Гані, Охрименко Андрій Олександрович,
Петришин Любомир Богданович, Петришин Михайло Любомирович,
Пушкар Олександр Іванович, Потрашкова Людмила Володимирівна,
Свердло Тамара Олексіївна, Смірнов Олексій Анатолійович,
Ушакова Ірина Олексіївна, Фонта Наталля Григорівна,
Фразе-Фразенко Олексій Олексійович, Хорошко Володимир Олексійович,
Хохлачова Юлія Євгенівна, Шматко Олександр Віталійович,
Щербаков Олександр Всеволодович**

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Монографія

За ред. д.-ра економ. наук, професора В.С. Пономаренко

Підписано до друку30.03.2015. Формат 60×84/16. Папір офсетний.
Гарнітура «Times New Roman». Друк – різограф. Ум.-друк. арк. – 23,5.
Ціна договорна Наклад 300 прим. Зам. 0330/7-15

Видавництво ТОВ "Щедра садиба плюс"
Свідодство суб'єкта видавничої справи: серія ДК № 4666 від 18.12.2013 р.
61002, Україна, м. Харків, вул. Ярославська, 11

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009. 61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057) 778-60-34**
e-mail: **bookfabric@rambler.ru**