

## Литература

### Офлайн-публикации

1. Carvey H. Windows Forensics and Incident Recovery, 2004.
2. Jones R. Internet Forensics, 2005.
3. Solomon M., Broom N., Barrett D. Computer Forensics Jumpstart, 2004.
4. Mohay G., Anderson A., Collie B., de Vel O., McKemmish R. Computer and Intrusion Forensics, 2003.
5. Caloyannides M.A. Privacy Protection and Computer Forensics (Second Edition). — «Artech House Publishers», 2004.
6. Casey E. Digital Evidence and Computer Crime (2nd Edition), 2004.
7. Good Practice Guide for computer based Electronic Evidence, (версия 3.0). Association of Chief Police Officers (ACPO). Великобритания, 2006.
8. Вехов В.Б., Илюшин Д.А., Попова В.В. Тактические особенности расследования преступлений в сфере компьютерной информации: Научно-практическое пособие. 2-е изд. — М.: ЛексЭст, 2004.
9. Завидов Б.Д. Обычное мошенничество и мошенничество в сфере высоких технологий. М., 2002.
10. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001.
11. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response — Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800-86. 2006.
12. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. акад. Б.П.Смагоринского. — М.: Право и Закон, 1996.
13. Войскунский А.Е. Психологические исследования феномена интернет-аддикции // 2 я Российская конференция по экологической психологии. Тезисы.
14. Гуманитарные исследования в Интернете. М., 2000.
15. Мир Интернет. 1999, №9.
16. Рабовский С.В. Социальные аспекты информатизации российского общества. М., 2001.
17. Митрохина Е. Информационные технологии, Интернет, интернет-зависимость // журнал «Наука, политика, предпринимательство». 2004, №1. С. 83.

18. Schneier B. Applied Cryptography. Protocols, Algorithms, and Source Code in C. «John Wiley & Sons, Inc», 1996.
19. Федотов Н.Н. DoS-атаки в Сети. Введение, текущая практика и прогноз // журнал «Документальная электросвязь». 2004, №13 (<http://www.rtfcomm.ru/about/press/pa/?id=429>).
20. Фирсов Е.П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов / Монография под науч. ред. д.ю.н. проф. Комисарова В.И. — М.: Юрлитинформ, 2004.
21. Середа С.А., Федотов Н.Н. Расширительное толкование терминов «вредоносная программа» и «неправомерный доступ». // Закон, июль, 2007, с. 191.
22. Daigle L. RFC-3912 «WHOIS Protocol Specification», 2004.
23. Dagon D., Gu G., Zou C., Grizzard J., Dwivedi S., Lee W., Lipton R. A Taxonomy of Botnets ([http://www.math.tulane.edu/~tcsem/botnets/ndss\\_botax.pdf](http://www.math.tulane.edu/~tcsem/botnets/ndss_botax.pdf)).
25. Серго А.Г. Доменные имена. — М.: Бестселлер, 2006.
26. Mockapetris P. RFC-1034 «Domain names — concepts and facilities», 1987.
27. Mockapetris P. RFC-1035 «Domain names — implementation and specification», 1987.
28. Стандарт RFC-3986 «Uniform Resource Identifier (URI): Generic Syntax».
29. Arends R., Austein R., Larson M., Massey D., Rose S. Стандарт RFC-4034 «Resource Records for the DNS Security Extensions», 2005.
30. Fielding R., Mogul J., Masinter L., etc. RFC-2616 «Hypertext Transfer Protocol — HTTP/1.1», 1999.
31. Resnick P. (editor) Стандарт RFC-2822 «Internet Message Format», 2001.
33. Rivest R. RFC-1321. «The MD5 Message-Digest Algorithm», 1992.
34. NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.
35. Schneier B. Cyberwar // Crypto-Gram Newsletter, January 15, 2005.
36. Хофман Б. Терроризм взгляд изнутри = Inside terrorism [пер. с англ.]. — М.: Ультра-культура, 2003.
37. Почепцов Г.Г. Информационные войны. — М.: Рефл-бук, К., Вак-лер, 2000.
38. Панарин И. Технология информационной войны. Издательство «КСП+», 2003.
39. Benton D., Grindstaff F. Practical Guide to Computer Forensics: For Accountants, Forensic Examiners and Legal Professionals. «BookSurge Publishing», 2006.
40. Соловьев Л.Н. Классификация способов совершения преступлений, связанных с использованием и распространением вредоносных программ для ЭВМ.

41. Крылов В.В. Расследование преступлений в сфере информации. — М.: Городец, 1998.
42. Экспертизы на предварительном следствии: Краткий справочник / Под общ. ред. В.В.Мозякова. — М.: ГУ ЭКЦ МВД России, 2002.
43. Иванов Н.А. Применение специальных познаний при проверке «цифрового алиби» // журнал «Информационное право», 2006. №4 (7).
45. RFC-3954 «Cisco Systems NetFlow Services Export Version 9», 2004.
46. RFC-3917 «Requirements for IP Flow Information Export (IPFIX)», 2004.
47. Mikkilineni A.K., Chiang P.-J., Ali G.N., Chiu G.T.-C., Allebach J.P., Delp E.J. Printer Identification based on textural features / Proceedings of the IS&T's NIP20: International Conference on Digital Printing Technologies, Volume 20, Salt Lake City, UT, October/November 2004, pp. 306-311.
48. Горбатов В.С., Полянская О.Ю. Мировая практика криминализации компьютерных правонарушений. — М.: МИФИ, 1996.
49. Strombergson J., Walleij L., Faltstrom P. RFC-4194 «The S Hexdump Format», 2005.
50. Albert J. Marcella Jr., Robert S. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. «Greenfield», 2002.
51. Jansen W., Ayers R. Guidelines on PDA Forensics: Recommendations of the National Institute of Standards and Technology (NIST), Publ. SP-800-72, 2004.
52. Oseles L. Computer Forensics: The Key to Solving the Crime, 2001.
53. Feather C. RFC-3977 «Network News Transfer Protocol (NNTP)», 2006.
54. Adams R., Horton M. RFC-1036 «Standard for Interchange of USENET Messages», 1987.
55. Lonvick C. RFC-3164 «The BSD syslog Protocol», 2001.
56. Casey E. Practical Approaches to Recovering Encrypted Digital Evidence, 2002.
57. Jones K.J., Bejtlich R., Rose C.W. Real Digital Forensics: Computer Security and Incident Response. «Addison-Wesley Professional», 2005.
58. Bartle R.A. Pitfalls of virtual property, 2004 (<http://www.themis-group.com/uploads/Pitfalls%20of%20Virtual%20Property.pdf>).
59. Bisker S., Butterfield J., Jansen W., Kent K., Tracy M. Guidelines on Electronic Mail Security (Draft). Recommendations of the National Institute of Standards and Technology // NIST Publ. 800-45A.
60. Ayers R., Jansen W., Cilleros N., Daniellou R. Cell Phone Forensic

- Tools: An Overview and Analysis / National Institute of Standards and Technology, NISTIR 7250, 2005.
61. Hare R.D., Hart S.D., Harpur T.J. Psychopathy and the DSM-IV Criteria for Antisocial Personality Disorder.
62. Moriarty L. Controversies in Victimology. «Anderson Publishing», Cincinnati, 2003.
63. Doerner W., Lab S. Victimology (4th edition). — «LexisNexis Anderson», Cincinnati, 2005.
64. Mohay G., Anderson A., Collie B., de Vel O., McKemmish R. Computer and Intrusion Forensics. — «Artech House», Boston, London, 2003.
65. Sriyith K.N. Analysis of Defacement of Indian Web Sites // First Monday, volume 7, number 12 (December 2002).
66. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006.
67. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: Солон-Пресс, 2002.
68. Торвальд Ю. Сто лет криминалистики. — М.: Прогресс, 1974.
70. Серeda С.А., Федотов Н.Н. Ответственность за распространение вредоносных программ для ЭВМ // Право и экономика. 2007, №3. С. 50-55.
71. Programming PHP. «O'Reilly», 2006.
72. Scambray J. Web Applications (Hacking Exposed). «McGraw-Hill», 2002.
73. Phishing Exposed. «Syngress Publishing», 2005.
74. Luna J.J. How to Be Invisible: The Essential Guide to Protecting Your Personal Privacy, Your Assets, and Your Life. «Thomas Dunne Books», 2004.
75. Anzaldua R., Volonino L., Godwin J. Computer Forensics: Principles and Practices. «Prentice Hall», 2006.
76. Шапиро И. Введение в типологию либерализма // журнал «Полис». 1994, №3. С. 7-12.
77. Быков П. Перспективы либерального консерватизма в России // журнал «Эксперт». 2007, №13.
78. Baker F., Foster B., Sharp C. RFC-3924: Cisco Architecture for Lawful Intercept in IP Networks. 2004.
79. Horrigan J.B. Home Broadband Adoption 2006. Pew Internet & American Life Project, 2006, 80.
80. Postel J. RFC-792: Internet Control Message Protocol. 1981, 81.
81. Серeda С.А., Федотов Н.Н. Сложности толкования терминов «вредоносная программа» и «неправомерный доступ» // журнал «Российская юстиция». 2007, №2. С. 58-62.
82. Hoglund G., McGraw G. Exploiting Software: How to Break Code. «Addison Wesley», 2004.

83. Hoglund G., Butler J. Rootkits: Subverting the Windows Kernel. «Addison Wesley», 2005.
84. Ayers R., Jansen W. An Overview and Analysis of PDA Forensic Tools, Digital Investigation // The International Journal of Digital Forensics and Incident Response, Volume 2, Issue 2, April 2005.
85. Губанов В.А., Салтевский М.В., Щербаковский М.Г. Осмотр компьютерных средств на месте происшествия: Методические рекомендации. — Харьков: Академия правовых наук Украины, НИИ изучения проблем преступности, 1999.
86. Михайлов И.Ю. Методические рекомендации: Носители цифровой информации (обнаружение, изъятие, назначение компьютерно-технической экспертизы). — Курган: ЭКЦ при УВД Курганской области, 2003.
87. Spivey M.D. Practical Hacking Techniques and Countermeasures. «AUERBACH», 2006.
88. Азимов Э.Л., Шукин А.И. Словарь методических терминов (теория и практика преподавания языков). — СПб.: Златоуст, 1999.
89. Prosis C., et all. Incident Response and Computer Forensics (Second Edition), 2001.
90. Middleton B. Cyber Crime Investigator's Field Guide (Second Edition). «Auerbach», 2004.
91. Steel C. Windows Forensics: The Field Guide for Corporate Computer Investigations. «Wiley», 2006.
92. Ayers R., Jansen W. Forensic Software Tools for Cell Phone Subscriber Identity Modules // Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL), April 2006.
93. Jansen W., Ayers R. PDA Forensic Tools: An Overview and Analysis. NISTIR 7100, 2004.
94. Компьютерное пиратство: методы и средства борьбы: Методическое пособие. 8-е изд. — М.: НП ППП, 2005.
95. Lo C. «ATM Cameras Found by Chance» // South China Morning Post, 9 January 2004, p. 1.
96. Shepardson D. «Police Accuse Man of ATM Scheme» // The Detroit News, 5 December 2003.
97. Taylor N. «Bank Customers Warned of Hi-Tech Thievery at ATMs» // South China Morning Post, 16 December 2003, p. 3.
98. Федотов Н.Н. Реликтовое право // Закон и право. №4, 2007, с. 18-20.

### Интернет-публикации

- W01. Cellular/Mobile Phone Forensics.  
http://www.e-evidence.info/cellular.html

- W02. Computer Forensic Software Tools Downloads.  
http://www.forensic-computing.ltd.uk/tools.htm
- W03. Khalid. Introduction to Digital Archeology.  
http://baheyeldin.com/technology/digital-archeology.html
- W04. Пятиизбянцев Н. Проблемы уголовно-правовой борьбы с преступлениями в области банковских карт.  
http://bankir.ru/analytics/Ur/36/66441
- W05. Безмалый В.Ф. Мошенничество в Интернете // «Security Lab», 6 декабря 2006.  
http://www.securitylab.ru/contest/280761.php
- W06. Reverse IP DNS Domain Check Tool.  
http://www.seologs.com/ip-domains.html
- W07. Фальшивый сайт прокуратуры сделал Rambler? (обзор публикаций прессы). Компромат.Ru.  
http://compromat.ru/main/internet/gprfl.htm
- W08. В Интернете появился поддельный сайт Генпрокуратуры РФ // NewsRU. Новости России, 1 октября 2003.  
http://www.newsru.com/russia/01oct2003/genprocuratura.html
- W09. Поддельный сайт Генпрокуратуры предвосхищает действия настоящей Генпрокуратуры // NewsRU. Новости России, 3 октября 2003.  
http://www.newsru.com/russia/03oct2003/site.html)
- W10. Википедия. Список файловых систем.  
http://ru.wikipedia.org/wiki/Список\_файловых\_систем
- W11. Википедия. Сравнение файловых систем.  
http://ru.wikipedia.org/wiki/Сравнение\_файловых\_систем
- W12. Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4 / National Institute of Justice, U.S. Department of Justice, 2004. Этот и другие отчёты NJI о тестировании доступны в Интернете:  
http://www.ojp.usdoj.gov/nij/pubs-sum/203095.htm  
http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm  
http://www.ojp.usdoj.gov/nij/pubs-sum/200032.htm  
http://www.ojp.usdoj.gov/nij/pubs-sum/199000.html  
http://www.ojp.usdoj.gov/nij/pubs-sum/196352.htm
- W13. Википедия. Информационная война.  
http://ru.wikipedia.org/wiki/Информационная\_война
- W14. США получили секретные коды для слежки за гражданами мира через принтеры.  
http://vkabinet.ru/articles.php?aid=1  
http://www.newsru.com/world/20oct2005/printer.html#1
- W15. DocuColor Tracking Dot Decoding Guide.  
http://www.eff.org/Privacy/printers/docucolor/

- W16. Is Your Printer Spying On You?  
<http://www.eff.org/Privacy/printers/>
- W17. Purdue Sensor and Printer Forensics (PSAPF).  
<http://cobweb.ecn.purdue.edu/~prints/>
- W18. Википедия: Hex dump.  
<http://en.wikipedia.org/wiki/Hexdump>
- W19. Спецификация алгоритма «yEnc».  
<http://www.yenc.org/>
- W20. Перечень и сравнительные характеристики клиентов файлообменных сетей.  
[http://en.wikipedia.org/wiki/Comparison\\_of\\_file\\_sharing\\_applications](http://en.wikipedia.org/wiki/Comparison_of_file_sharing_applications)
- W21. P2P-сервисы выходят на следующий этап своего развития // «Security Lab», 3 ноября 2006  
<http://www.securitylab.ru/news/276373.php>
- W22. Тутубалин А. RBL: вред или польза? // Электронный журнал «Спамтест»  
<http://www.spamtest.ru/document.html?pubid=22&context=9562>
- W23. Федотов Н.Н. О «черных списках» фильтрации почты // Электронный журнал «Спамтест».  
<http://www.spamtest.ru/document.html?pubid=8&context=9562>
- W24. Собоцкий И.В. О доказательственном значении лог-файлов // «Security Lab», 25 июля 2003.  
<http://www.securitylab.ru/analytics/216291.php>
- W25. Sarangworld Traceroute Project Known Hostname Codes.  
<http://www.sarangworld.com/TRACEROUTE/showdb-2.php3>
- W26. Fingerprint Sharing Alliance.  
<http://www.arbornetworks.com/fingerprint-sharing-alliance.php>
- W27. Antisocial Personality Disorder for professionals. Armenian Medical Network.  
[http://www.health.am/psy/more/antisocial\\_personality\\_disorder\\_pro/](http://www.health.am/psy/more/antisocial_personality_disorder_pro/)
- W28. Forensic Examination of Computers and Digital and Electronic Media (IACIS).  
<http://www.iacis.info/iacisv2/pages/forensicprocprint.php>
- W29. Собоцкий И.В. Организация технико-криминалистической экспертизы компьютерных систем // «Security Lab», 10 ноября 2003.  
<http://www.securitylab.ru/analytics/216313.php>

**Нормативные акты**

- L01. Постановление Правительства РФ от 27 августа 2005 г. №538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» // Собрание законодательства Российской Федерации, №36, 05.09.2005, ст. 3704.
- L02. Постановление Пленума Верховного Суда Российской Федерации №15 от 19 июня 2006 г. «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах».
- L03. Правила регистрации доменных имен в домене RU — нормативный документ Координационного центра национального домена сети Интернет, утвержден решением П2-2.1, 4.1/06 от 24.04.2006.
- L04. Федеральный закон «Об оценочной деятельности в Российской Федерации» от 29 июля 1998 г. (№135-ФЗ).
- L05. Закон РФ «О коммерческой тайне» (№98-ФЗ).