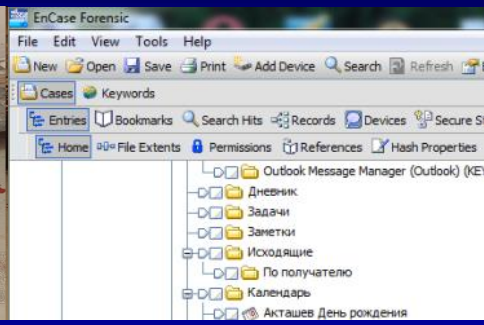
конференция
РусКрипто

22 – 25 марта 2016 года
Солнечный Park Hotel & SPA

Цифровая криминалистика и расследование инцидентов



Исследования цифровой информации: состояние, проблемы, решения

Яковлев Алексей Николаевич, заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики Следственного комитета России; доцент кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы МГТУ им. Н.Э. Баумана

Заключение экспертов

№ 2471/20

Составлено " 15" апреля 1997 г.

"20" января 1997 г. в Центральную Санкт-Петербургскую лабораторию судебной экспертизы МЮ РФ от инспектора ОТР Пулковской таможни [redacted] М.Л. при постановлении от "16" января 1997 г. поступили для производства судебно-кибернетической экспертизы:

а) Чип-карты для таксофона различного достоинства - 7 штук.

б) Техническая документация (описанная в тексте исследования):

1. Описание технологии используемой в чип-картах;
2. Техническое описание GPM 103;
3. Общее описание карт предоплаты;
4. Руководство по эксплуатации GNT 807;
5. Технические условия на таксофон;

в) Копии письменных документов:

6. Техническое описание чип-карты таксофона GNT-807;
7. Письмо ЛОНИИС от 11.01.97;
8. Письмо Процессингового центра СПб банка СБ РФ № 22/224 от 06.01.97;
9. Акт консультации ТПП СПб № 05-1302 от 07.12.94.

ЗАКЛЮЧЕНИЕ ЭКСПЕРТА

№ 1 от 02 марта 1998 г.

Сотрудники кафедры Управления и информационно-технического обеспечения ОВД Саратовского юридического института МВД РФ Яковлев А.Н., имеющий высшее образование, специальность - математик, стаж работы со средствами вычислительной техники 13 лет, и Гортинский А.В., имеющий высшее образование, специальность - математик, стаж работы со средствами вычислительной техники 12 лет, на основании постановления о назначении экспертизы, вынесенного 02.02.98 г. следователем прокуратуры г. Саратова [redacted] С.В. по уголовному делу № 3804, произвели компьютерно-техническую экспертизу компьютерной техники.

Обстоятельства дела:

13 и 15 января 1998 г. [redacted] и [redacted], вступив в предварительный сговор, на своем рабочем месте в поселке Сторожовка Татищевского района Саратовской области изготавливали в целях сбыта, а в дальнейшем сбывали поддельные денежные купюры достоинством 50 рублей. 16 января 1998 г. в ходе обыска в поселке Сторожовка Татищевского района г. Саратова в помещении бухгалтерии УРВР-2 был изъят комплект компьютерной техники.

На экспертизу представлен:

1. Комплект компьютерной техники в составе: монитор SAMSUNG Sync Master 3NE, системный блок "Вист", принтер EPSON Color 600, сканер HP Scanjet 5P, клавиатура SMART - 104.

←EОткрытое акционерное общество энергетики и электрификации
"САРАТОВЭНЕРГО"←F

Зарегистрировано Администрацией г.Саратова 05.03.93 г. Рег.N 01091371.

410720, г.Саратов
ул.Чернышевского, 124

Выписка из реестра акционеров

[redacted] Алексей Валерьевич

Реестровый номер N 001283 Филиал Саратовская ГРЭС-ТЭЦ1
Паспорт N [redacted] Кировским РОВД г Саратова [redacted]
Адрес 410005 г Саратов ул [redacted] кв 159

Владеет ценными бумагами на 10.09.97 г:

Название ценных бумаг	Номинальная стоимость,руб.	Количество,шт.
Акции привилегированные 60-1-П-193	250	244
Акции обыкновенные 60-1-П-193	250	274
Акции привилегированные 60-1-227	250	306364
Акции обыкновенные 60-1-227	250	393128

Держателем реестра является АО "Саратовэнерго".

Начальник отдела акционирования
и ценных бумаг _____

М. П.

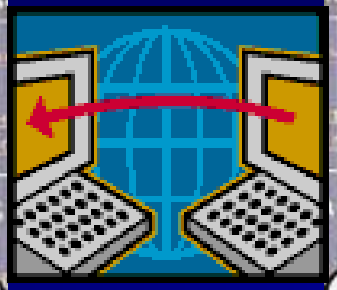
Ответственный за ведение
реестра _____

ПРИМЕЧАНИЕ: Выписка из реестра не является ценной бумагой. Передача ее от одного лица другому не означает совершение сделки и не влечет переход прав на акции.

-104-

Пользователь ПК (15.02.2005 23:33:11) :	***у тебя что поверменка?***
[redacted] (15.02.2005 23:33:18) :	нет
Пользователь ПК (15.02.2005 23:34:55) :	***хочешь я тебе оверту подарю старт***
[redacted] (15.02.2005 23:35:18) :	давай !
Пользователь ПК (15.02.2005 23:36:22) :	***Entry Name : rty Phone / Host : p470333 User Name : 03-142906@55 Password : 141-XSJW-531 Domain : Owner : System User Profile : Пользователь***
[redacted] (15.02.2005 23:40:14) :	ну что подаришь?
Пользователь ПК (15.02.2005 23:40:22) :	***только что же скопировал***
[redacted] (15.02.2005 23:40:31) :	у меня лаги !

Пользователь ПК (15.02.2005 23:40:35) :	***мля***
Пользователь ПК (15.02.2005 23:40:44) :	***_банан_ (11:36 PM) : Entry Name : rty Phone / Host : p470333 User Name : 03-142906@55 Password : 141-XSJW-531 Domain : Owner : System User Profile : Пользователь***
[redacted] (15.02.2005 23:41:03) :	ок !!! а там что джокер?
Пользователь ПК (15.02.2005 23:41:17) :	***не знаю...там 80 руб осталось***
[redacted] (15.02.2005 23:41:59) :	это не опасно?
[redacted] (15.02.2005 23:42:41) :	)))
[redacted] (15.02.2005 23:42:58) :	ладно щас переконектюсь...
Пользователь ПК (15.02.2005 23:42:58) :	***пока никто не жаловался..как написано в договоре..рльзователь сам несет ответственность за сохранность своих личных данных и любой ущерб причиненный в результате их утраты провайдером не компенсируется***



Российские хакеры испугали Европу на $4 милл

ДОПОМАЛИСЬ

Хакер — это не круто. Это 8 лет колонии

К восьми годам колонии строгого режима приговорены российские хакеры, вымогавшие деньги у Интернет-компаний Великобритании и Северной Ирландии.

Балаковский районный суд признал трех жителей Саратовской области, Астрахани и Санкт-Петербурга виновными по одиннадцати статьям Уголовного кодекса.

Процесс по делу компьютерных взломщиков длился больше года. Одним из авторов вредоносной программы стал студент четвертого курса Балаковского института техники Иван Максаков. Юноша вырос в благополуч-

В расследовании принимали участие правоохранительные органы Великобритании, США, Латвии, России и Интерпол. Как говорят специалисты управления «К», Иван попался случайно: выпил пива, вышел в Интернет со

8 ЛЕТ строгого режима от букмекеров

«Подарил» хакерам суд города Балаково

В Саратовской области оглашен приговор по так называемому «делу хакеров», молодых людей, обвиняемых в вымогательстве денег у английских букмекеров.

Как установил суд, Иван Максаков (1984 г.р., житель г. Балаково), Александр Петров (1982 г.р., Астрахань) и Денис Степанов (1981 г.р., Санкт-Петербург) входили в группу злоумышленников, которая вымогала деньги у девяти крупнейших британских букмекерских интернет-компаний.

По версии следствия, Максаков, Петров и Степанов, знакомые между собой только по сетевым псевдонимам, договорились о совместном участии в «заговоре хакеров» и заражали специально написанными вирусами сотни компьютеров, подключенных к сети Интернет, а затем, с помощью этих компьютеров, управляемых также по сети, забрасывали серверы букмекеров огромным количеством ложных запросов. При этом хозяева зараженных компьютеров ни о чем не подозревали. А взятые «на мушку» серверы не успевали обработать запросы и «висли». После этого ребята посылали владельцам серверов письма по электронной почте с требованием перечислить на определенные счета в Латвии суммы (в разных случаях — 10, 15, 40 тысяч долларов). Полученные средства переводились в Пятигорск, а оттуда по системе WEB-money распределялись между участниками «заговора хакеров». D-DoS атаки и вымогательства продолжались с октября 2003-го по июнь 2004 года.

В одном случае эта затея увенчалась успехом. После неоднократных атак на сетевой ресурс www.canbet.com (одна из которых происходила во время популярных скачек на «кубок Бридерса») компания Canbet Sports Bookmakers UK Ltd ответила согласием на письмо о немедленной выплате 40 тысяч долларов США. Очень скоро на служебный e-mail пришел список из двух десятков фамилий граждан Латвии, которым надлежало отправить требуемую сумму денег, разбив ее на части. Перечисление предлагалось провести по международной системе денежных переводов «Вестерн Юнион». Деньги были перечислены, но D-DoS атаки не прекратились. После этого случая девять крупных английских букмекерских интернет-компаний — Canbet Sports Bookmakers UK Ltd, Betinternet.com Plc, Stanley Racing Limited, Ads Dot Com Ltd, Sportingbet Plc, Eurobet Uk Ltd, The Sporting Exchange Ltd, Blue Square Ltd и British Sky Broadcasting — обратились в полицию.

Британская спецслужба — Национальный департамент по борьбе с преступлениями в сфере высоких технологий — совместно с МВД России провели оперативное мероприятие, которое завершилось задержанием хакеров летом 2004-го. Предварительное следствие и суд тянулись два года. Совокупный ущерб, понесенный букмекерами в результате D-DoS атак, оценен в сумму более 5 миллионов долларов.

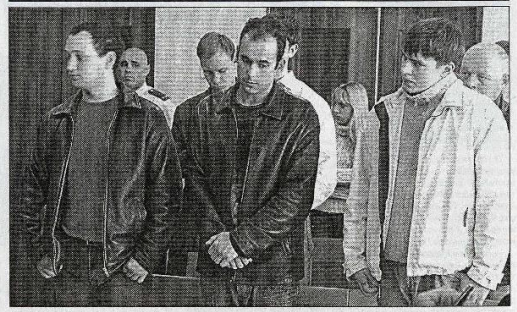
Следственные мероприятия и судебные баталии по делу тянулись два года. Приговор судья зачитывал полдня, заговариваясь и путаясь в специфических компьютерных терминах. Когда стало ясно, что всем подсудимым назначен реальный срок, в зал вошел конвой и надел на подсудимых наручники. Несмотря на то, что один из хакеров, Максаков, активно сотрудничал со следствием, вся тройка получила одинаковое наказание — по 8 лет лишения свободы с отбыванием срока в колонии строгого режима. Срок сложился из наказаний по двум статьям УК РФ: 163 «Вымогательство» и 273 «Создание, использование, распространение вредоносных программ для ЭВМ». Обвинение по статье 165 «Причинение имущественного ущерба» (без признаков хищения) суд отклонил, так как эта статья предусматривает введение в заблуждение потерпевших, чего в действительности не было. Дополнительно к основному наказанию каждому хакеру был назначен штраф — 100 тысяч рублей.

Адвокаты подсудимых немедленно после окончания процесса заявили о своем намерении обжаловать приговор, вплоть до Европейского суда по правам человека.

Однако государственный обвинитель Антон Пахомов сразу же после оглашения приговора сообщил представителям СМИ, что и он лично, и представители спецслужб Великобритании очень довольны вынесенным решением суда.

Осужденных молодых людей прокурор также назвал «международными компьютерными террористами».

Еще один предполагаемый компаньон хакеров по «компьютерному ракету» Тимур Арутчев (1973 г.р. из Пятигорска) был ранее также взят под стражу в зале суда, в который пришел в качестве свидетеля. Дело Арутчева выделено в отдельное производство.



Иван ИВАНОВ, Роман ОБНОРСКИЙ

1-я группа объектов исследования:

серверы, «обычные» компьютеры, ноутбуки
(любые операционные системы)

2-я группа объектов исследования:

SYMBIAN maemo ANDROID

Windows phone MeeGo™

webOS iOS

bada BlackBerry

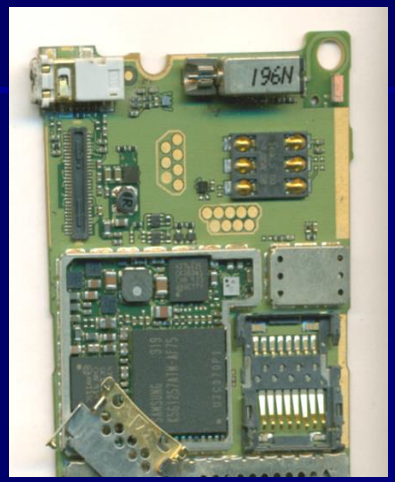
hp palm webOS

ANDROID

BlackBerry™

мобильные устройства (планшеты, мобильные телефоны: любые операционные системы)

3-я группа объектов исследования:

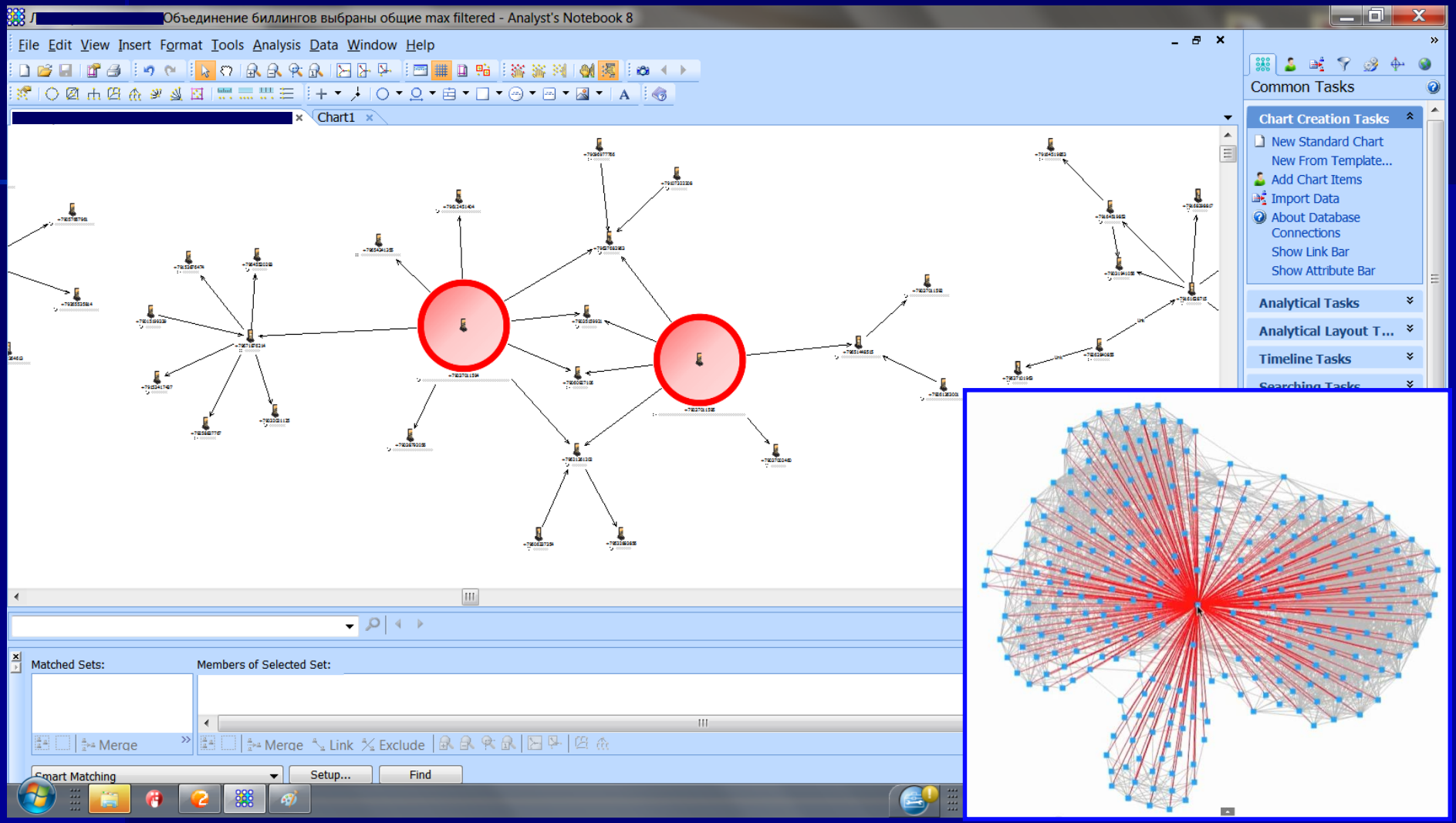


повреждённые компьютерные устройства, мобильные телефоны

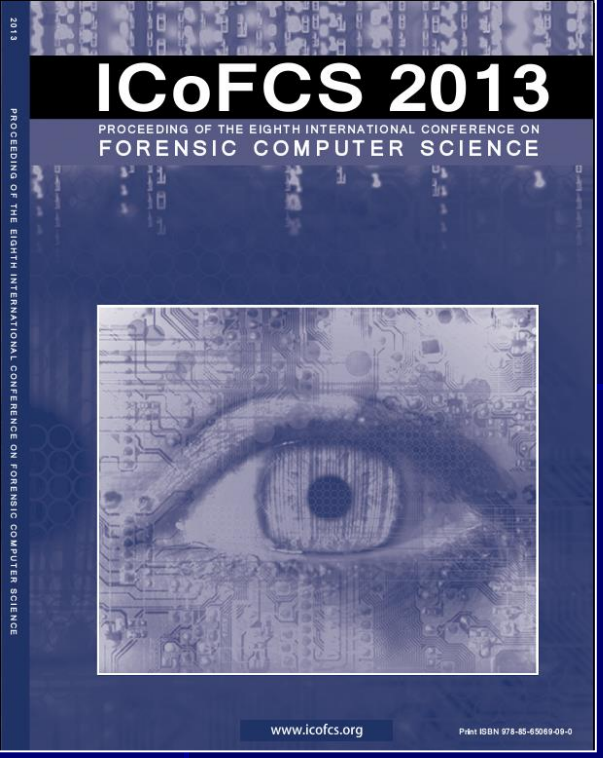
4-я группа объектов исследования:

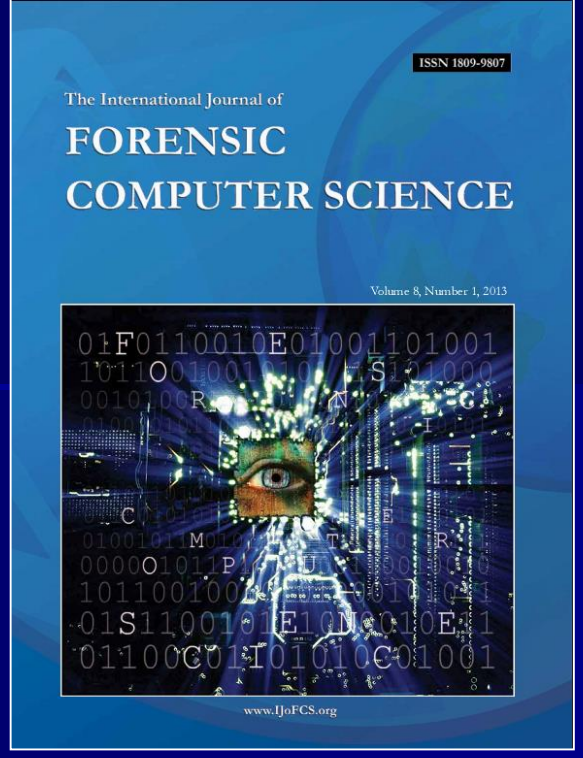
фото-, видеотехника, автомобильные, стационарные видеорегистраторы

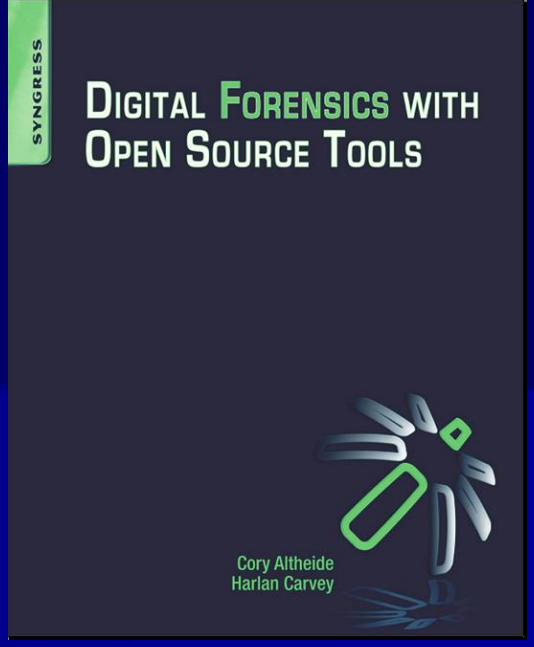
5-я группа объектов исследования:

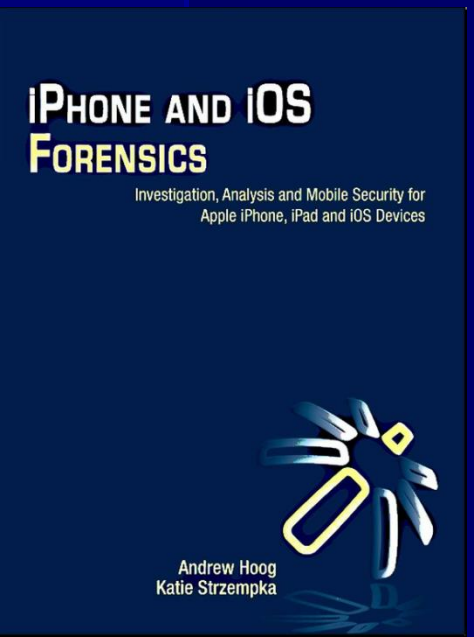


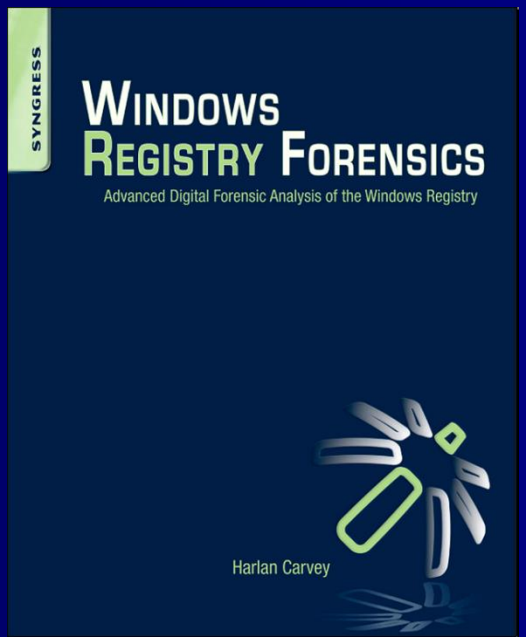
массивы структурированной информации (соединения абонентских устройств, данные системы «Поток», социальные сети и т.п.)











Цифровая криминалистика – международный вид исследований

Судебная экспертиза цифровых устройств (digital forensic):

- компьютерная экспертиза (computer forensics);
- экспертиза компьютерной сети (network forensics);
- экспертиза баз данных (database forensics);
- экспертиза мобильных устройств (mobile device forensics).

Федеральные ведомства и иные организации, выполняющие компьютерно-технические экспертизы

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

- Министерство юстиции Российской Федерации,
- Министерство внутренних дел Российской Федерации,
- Федеральная служба безопасности Российской Федерации,
- Федеральная служба Российской Федерации по контролю за оборотом наркотиков,
- Следственный комитет Российской Федерации

ЧАСТНЫЕ СТРУКТУРЫ

- Форензик-компании

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.3-20ХХ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

СБОР И АНАЛИЗ ТЕХНИЧЕСКИХ ДАННЫХ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

РОССТАНДАРТ
ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ 134 «СУДЕБНАЯ ЭКСПЕРТИЗА» (ТК 134 «СУДЕБНАЯ ЭКСПЕРТИЗА»)
Хохловский переулок, д.13, стр.2, г. Москва, 109028,
тел.(495) 181-57-57 *3601, nmo@sudexpert.ru

15.10.2015 № 1-73
На № _____ от _____

Уважаемый [redacted]!

Приглашаю представителей Вашего управления принять участие в заседаниях рабочих групп при Техническом комитете по стандартизации 134 «Судебная экспертиза» по разработке проектов национальных стандартов, которые состоятся в ФБУ РФЦСЭ при Минюсте России по адресу: г. Москва, Хохловский пер., д. 13, стр. 2, 4 этаж, каб. 415.

Тематика и время заседаний приведены ниже:

- компьютерно-техническая экспертиза: термины и определения – 19 октября в 15.00;

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р

Стандартизация в Российской Федерации

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Настоящий проект стандарта не подлежит применению

до его утверждения

ВОПРОСЫ ?

Яковлев Алексей Николаевич, заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики Следственного комитета России; доцент кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы МГТУ им. Н.Э. Баумана