МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Юридический факультет
Кафедра криминалистики

Современная криминалистика: проблемы, тенденции, перспективы

Материалы
Международной научно-практической конференции,
посвященной 90-летию со дня рождения
Заслуженного деятеля науки РФ, Заслуженного юриста РСФСР,
доктора юридических наук, профессора
Николая Павловича Яблокова

Москва, 22 декабря 2015 г.

МАКС ПРЕСС

МОСКВА – 2015

ISBN 978-5-317-05163-1

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Юридический факультет

Кафедра криминалистики

Современная криминалистика: проблемы, тенденции, перспективы

Материалы
Международной научно-практической конференции,
посвященной 90-летию со дня рождения
Заслуженного деятеля науки РФ, Заслуженного юриста РСФСР,
доктора юридических наук, профессора
Николая Павловича Яблокова

Москва, 22 декабря 2015 г.

МАКС ПРЕСС

МОСКВА – 2015

УДК 343.9
ББК 67.52
С56

Редактор-составитель: *М.А. Лушечкина*

Статьи представлены в авторской редакции

Современная криминалистика: проблемы, тенденции, перспективы:
С56 Материалы Международной научно-практической конференции, посвященной 90-летию со дня рождения Заслуженного деятеля науки РФ, Заслуженного юриста РСФСР, доктора юридических наук, профессора Николая Павловича Яблокова. Москва, 22 декабря 2015 г. / Ред.-сост. М.А. Лушечкина. – М.: МАКС Пресс, 2015. – 511 с.
ISBN 978-5-317-05163-1

В опубликованных статьях криминалисты из России, Беларуси, Казахстана, и Украины рассматривают актуальные проблемы развития криминалистики по всем ее разделам: теории и методологии, криминалистической техники, криминалистической тактики, методики расследования отдельных видов преступлений, а также обсуждают вопросы процессуального регулирования криминалистической деятельности, проблемы использования специальных знаний и развития судебной экспертизы. Содержание сборника отражает новые подходы в развитии криминалистики как науки, практической деятельности и учебной дисциплины.

УДК 343.9
ББК 67.52

Modern forensic science: problems, trends, perspectives: International science-and-practice conference dedicated to 90th anniversary of professor N.P. Yablokov PhD. Moscow, December 22, 2015. / Ed. by M.A. Lushechkina. – M.: MAKS Press, 2015. – 511 p.

The following articles written by criminalists from Russia, Belarus, Kazakhstan and Ukraine deal with up-to-date problems of criminalistics in its every subdivision – criminalisitic technics, criminalistic tactics, theory and methodology, methods of criminal investigation. They also discuss issues of criminal procedure, usage of special knowledge and developing of forensic science. This digest explores the new approaches to criminalistics as scientific field, practice and study.

Электронное издание

ISBN 978-5-317-05163-1

VII. Методика расследования отдельных видов преступлений

Г.К. Авдеева, С.М. Бобрицкий

Инновации в борьбе с преступлениями, совершаемыми с использованием информационных технологий

В статье проводится анализ наиболее распространенных способов совершения преступлений, совершаемых с использованием информационных технологий. Особое внимание уделено преступлениям с использованием телекоммуникационных сетей. В зависимости от способов совершения таких преступлений систематизированы их следы. Указан оптимальный набор инновационных средств и методов борьбы с ними.

***Ключевые слова**: инновация, информационная технология, компьютер-ная преступность.*

G.K. Avdeeva S.M. Bobrytckiy

Innovations in the fight against crimes committed using information technology

In the article the analysis of the most common ways of committing crimes using information technologies. Special attention is paid to crimes using telecommunications networks. Depending on the methods of committing such crimes systematized their tracks. Specified optimal set of innovative means and methods of combating them.

***Keywords**: innovation, information technology, computer crime.*

Глобальная компьютеризация общества, развитие современных информационных технологий и телекоммуникационных систем привели к появлению новых средств и методов преступной деятельности. Это, в свою очередь, требует использования адекватных средств противодействия преступлениям, интенсивного внедрения инноваций в работу правоохранительных органов для своевременного выявления, квалифицированного расследования и профилактики преступлений в сфере использования информационных технологий. Однако, инновационными принято считать не любые нововведения, а лишь такие средства и методы, использование которых существенно повышают эффективность определенной деятельности.

Одним из способов совершения преступления в сфере компьютерных технологий является использование вредоносных программных продуктов. Зараженные «компьютеры-жертвы» помимо воли их владельцев становятся участниками botnet-сетей[1]. Кража личных персональных и коммерческих авторизационных данных пользователей, конфиденциальной информации, содержания ключей защиты, использование аппаратного ресурса «компьютера-жертвы» с последующей возможностью проведения DDoS-атак[2],

[1] Botnet – это компьютерная сеть, состоящая из некоторого количества компьютеров или устройств, поддерживающих сервис «клиент-сервер», с запущенными ботами – программным обеспечением, работающим автономно. Скрытно установленный бот на компьютере жертвы позволяет правонарушителю выполнять определенные действия с использованием ресурсов заражённого компьютера.

[2] DDoS-атака (атака типа «отказ в обслуживании», от англ.. Distributed Denial of Service) - атака одновременно с большого числа компьютеров на вычислительную систему с целью довести её до отказа, то есть, создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. – См.: Дремлюга Р.И. Интернет-преступность: моногр. / Р.И. Дремлюга. – Владивосток: Изд-во Дальневост. Ун-та, 2008. – С. 23.

несанкционированной рассылки сообщений и выполнения ложных транзакций[1] – вот далеко не полный перечень правонарушений, зафиксированных в банковской сфере Украины. Сегодня во всем мире количество преступлений с использованием телекоммуникационных сетей и сетевых технологий (киберпреступность) составляет 30-40% от общего количества преступлений, и их количество с каждым годом растет.[2] Сегодня в сети Интернет размещены предложения хакеров[3] по осуществлению DDoS-атак с указанием стоимости этого вида «услуг». В 2014 г. в г. Киеве задержан хакер, который совершал такие атаки на сайты украинских и зарубежных коммерческих структур по заказу конкурентов. В целях конспирации хакер общался с заказчиками через анонимные интернет-пейджеры, а денежные средства получал с помощью виртуальных платежных систем, зарегистрированных на подставных лиц.

Термин «преступления, совершаемые с использованием компьютерных технологий» охватывает все преступные действия, совершаемые с использованием этих технологий и те, которые посягают на компьютерную информацию. В криминалистическом аспекте такое определение позволило разработать инновационные типовые приемы, средства и методы обнаружения, фиксации и исследования компьютерной информации.

Одним из важнейших определяющих факторов в борьбе с данными преступлениями является область их совершения - киберпространство.[4] Компьютерная информация в зависимости от характера преступных деяний выступает как предмет посягательства и как область возможного сохранения следов преступной деятельности.

Специфическими свойствами компьютерной информации являются такие: отсутствие неразрывной связи с материальным носителем; динамичность, возможность мгновенного переноса в пространстве (в том числе из одной части земного шара в другую); возможность изменения и уничтожения информации любого объема за короткие промежутки времени (в т.ч. - при помощи удаленного доступа)[5]. Кроме того, все копии компьютерной информации (не зависимо от вида носителя) идентичны оригиналу. Такая специфика вызвала значительные сложности в расследовании киберпреступлений традиционными методами.

Следы с преступлений в сфере использования информационных технологий образуются в результате воздействия на компьютерную информацию путем внешнего доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Такими изменениями могут быть следы уничтожения, модификации, копирования информации, блокирования информационной системы. Следы изменений остаются на машинных носителях информации и отражают изменения в информации, которая в них хранится (по сравнению с исходным состоянием). Часто преступниками осуществляются модификации баз данных, программ, текстовых файлов, находящихся на стационарных и сменных носителях информации, предназначенных для

---

[1] Транзакция - банковская операция, состоящая в переводе денежных средств с одного счета на другой. – См.: Финансовый словарь. http://finance.sci-lib.com/

[2] «Русский» рынок компьютерных преступлений в 201 0 году: состояние и тенденции» Аналитический отчет. http://www.group-ib.ru

[3] Хакер [англ. hacker < to hack - рубить, прорубить] - компьютерный взломщик - тот, кто с помощью своего компьютера проникает в информационные сети банков, финансовых, промышленных и других организаций с целью получения необходимой информации, заражения этих сетей вирусом и др. – См.: Крысин Л.П. Толковый словарь иноязычных слов. – М.: Эксмо, 2008. – 944 с.

[4] Киберпространством называют сферу существования компьютерной информации, которая образована совокупностью средств компьютерной техники. - См: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж: Издательство Воронежского государственного университета, 2002. – С. 41.

[5] Криминалистика: Учебник / Под ред. Т.А. Седовой, А.А. Эксархопуло. – СПб.: Издательство «Лань», 2001. – С. 370.

многократной её перезаписи. Информация может сохранить следы ее частичного уничтожения или модификации (удаления из каталогов имен файлов, удаления или добавления отдельных записей, физического разрушения или размагничивания носителей). Информационными следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть обнаружены при экспертном исследовании компьютерного оборудования, протоколов работы операционных систем, приложений, антивирусных программ, программного кода и др.

Следы неправомерного доступа к информации можно обнаружить в сети Интернет, а затем, исходя из их признаков - установить исходное подключение и техническое средство, с которого совершалось данное правонарушение. Наименование и адрес интернет-провайдера[1], при помощи которого правонарушитель подключен к сети Интернет, можно получить через специальную службу Whois (в сети Интернет). В общедоступном сервисе по адресу www.ripe.net указан электронный адрес (IP) атакующего компьютера. Время работы пользователя в сети можно установить по специальному log-файлу (журналу). Дополнительные сведения о виде, порядке и времени подключений пользователя к сети Интернет и совпадение этих данных с log-файлом провайдера может служить весомым доказательством несанкционированного доступа в определенную компьютерную систему.

Определенную информационную ценность имеют SMS[2]-сообщения, которые автоматически фиксируются и накапливаются на сервере мобильного оператора. Изучение и анализ SMS-сообщений позволили в 2012 г. обезвредить организованную преступную группу, которая в Харькове, Киеве, Запорожье и др. городах Украины при помощи различных мошеннических действий и «театральных» представлений шантажировала состоятельных людей и в течение нескольких лет получала огромные суммы денежных средств. Данная преступная группа имитировала дорожно-транспортные происшествия, убийства по неосторожности, тяжкие телесные повреждения и др. Одни члены группы исполняли роль «трупов», другие – сотрудников правоохранительных органов. Организация каждого нового преступления сопровождалась сменой номеров мобильных телефонов каждого члена преступной группы. Членам данной группы было разрешено звонить с «рабочего» телефона только жертве преступления или друг другу и запрещено звонить родным и близким, однако однажды один из таких «артистов» позвонил своей супруге. Этот звонок, информацию о котором сотрудники правоохранительных органов получили от оператора мобильной связи, послужил отправной точкой к расследованию серии преступлений, совершенных по всей территории Украины.

Важную информацию можно получить при изучении данных электронной переписки и сервисов обмена мгновенными сообщениями. Во многих случаях именно эти следы позволяют установить организационные схемы преступлений. Так, анализ электронных сообщений и переписки в 2010 году на территории г. Харькова и других городов Украины позволил установить каналы поставки сырья для изготовления курительных смесей и энергетиков, основой которых служило синтетическое вещество «JWH» (при употреблении вызывает эффект, сравнимый с действием марихуаны), рекомендации по их производству, упаковке, особенностям реализации. Правоохранительными органами Украины пресечена преступная деятельность широкой сети реализации данной

[1] Интернет-провайдер (иногда просто провайдер; от англ. internet service provider, сокр. ISP - поставщик интернет-услуги) - организация, предоставляющая услуги доступа к сети Интернет и иные связанные с ней услуги.

[2] SMS [англ. Short Messaging Service - «служба коротких сообщений»] - технология, осуществлять прием и передачу коротких текстовых сообщений с помощью мобильного телефона. – См.: Англо-русский словарь по вычислительной технике и программированию (The English-Russian Dictionary of Computer Science): около 55 тыс. статей. – 8-е изд., испр. и доп. © ABBYY, 2008; © Масловский Е.К., 2008. [Электронная версия].

продукции. Лишь в г. Харькове сотрудниками правоохранительных органов выявлялось по 50-60 торговых точек в месяц, наибольшее количество которых находилось вблизи начальных школ.

Следы несанкционированного доступа к компьютерной информации содержатся в журналах операционных систем и отдельных приложений, которые могут создавать резервные копии файлов и файлы-отчеты, хранят информацию о последних проведенных операциях и выполненных программах, а также содержат иную информацию, имеющую значение для расследования. Следами, указывающими на посторонний доступ к информации, могут быть такие: переименование каталогов и файлов, изменение размеров и содержимого файлов, их атрибутов, появление новых каталогов, файлов, изменение времени последнего доступа к информации, её модификация и др.

В последние 2–3 года наблюдается рост правонарушений в системах дистанционного банковского обслуживания (ДБО). ДБО - это комплекс сервисов удаленного доступа клиентов к банковским услугам. При этом клиент удаленно (без визита в банк) передает необходимые распоряжения, используя информационные технологии.

Системы ДБО в Украине разделяются на такие виды: систему «Клиент Банк» (PC-banking, remote banking, direct banking, home banking); интернет-банкинг; мобильный банкинг. Мошенническая схема хищения денежных средств состоит из трех основных этапов: получение конфиденциальной информации для осуществления неправомерного доступа в систему ДБО, проведение мошеннической операции от имени пользователя с использованием его авторизационных данных и содержания ключей электронных средств защиты, «обналичивание» денежных средств. Для хищения персональных (авторизационных) данных пользователя системы ДБО (логина, пароля и ключей подписи) правонарушители используют специальное вредоносное программное обеспечение. Чаще всего это - модификации хорошо известных троянских программ с дополнительными функциями[1], позволяющими в последствии безвозвратно удалить троянскую программу без возможности её восстановления.

Условиями, способствующими хищению персональных (авторизационных) данных является не соблюдение субъектами предпринимательской деятельности, государственными учреждениями требований к нераспространению конфиденциальных данных (авторизационных данных пользователей Интернет-банкинга, содержания ключей электронных средств защиты), доступ посторонних лиц к конфиденциальной информации предприятия и недостаточная защита компьютерно-технических средств, которые работают в системах ДБО от внешней Интернет-среды локальной сети учреждения. Это дает возможность правонарушителям получать контроль над информацией и соединениями на интернет-ресурсах финансовых учреждений, манипулировать аппаратными возможностями компьютерно-технических средств с целью объединения их в botnet-сети для распространения спама[2] или организации DDoS-атак. Так в ряде случаев из анализа журналов операционной системы, журналов программ защиты операционной системы компьютера, фактического наличия вирусных и троянских кодов и программ становится понятным, что при подготовке преступления (например, ошибочной транзакции) преступники изучают время и технические возможности работы компьютерной системы потенциальной жертвы, блокируют ее работу в сети и «заражают» информацию пользователя с целью получения дистанционного контроля над определенными технологическими процессами. Самостоятельно пользователь (как правило, сотрудник бухгалтерии)

[1] Комплексное расследование мошенничества в системах интернет-банкинга. [Электронный ресурс]. – Режим доступа: http://www.group-ib.ru/images/media/Group-IB_AntiFraud.pdf.

[2] Спам (англ. spam) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать.

не в состоянии оценить опасность неожиданных задержек в работе компьютера и телекоммуникационных средств и не замечает загрузки не оригинальной web-страницы[1] ресурса банковского учреждения.

Для решения проблем борьбы с компьютерными преступлениями криминалистами исследуется технический характер их осуществления. Особое внимание уделено разработке новейших технических средств и приемов обнаружения, изъятия, фиксации и исследования следов преступлений с использованием компьютерных технологий. На сегодня разработано значительное количество эффективных современных средств поиска (восстановления) уничтоженной электронной информации. Судебными экспертами Украины используются такие программные продукты, как X-Ways Forensics, EnCase Forensics, FTK, AccessData Forensic Toolkit, Forensic Disk Decryptor, MailPro, FileLister и др.

Борьба с компьютерной преступностью не ограничивается установлением уголовной ответственности за конкретное совершенное преступление. Сегодня активно осуществляется построение международной системы борьбы с данными видами преступлений, объединяются необходимые кадры, разрабатываются методики, уточняются процедуры взаимодействия с международными структурами и правоохранительными органами других стран (в т.ч. – при помощи телекоммуникационных средств и систем).

А.В. Акчурин

О степени теоретической разработанности проблем расследования пенитенциарных преступлений*

В статье, предпринята попытка обобщения и систематизации разноаспектных разработок в области расследования преступлений, совершаемых осужденными в исправительных учреждениях. На основе данного анализа формулируется мнение автора об актуальных направлениях дальнейшего научного осмысления проблем расследования пенитенциарных преступлений.

***Ключевые слова**: расследование преступлений, осужденный, пенитенциарные преступления, исправительные учреждения.*

A. V. Akchurin

About degree of a theoretical readiness of problems investigations penitentiary crimes

In article, an attempt of generalization and systematization the various of development in the field of investigation of the crimes committed condemned in correctional facilities is made. Based on this analysis the opinion of the author on the actual directions of further scientific judgment of problems of investigation of penitentiary crimes is formulated.

***Keywords**: investigation of crimes, condemned, penitentiary crimes, correctional facilities.*

Начиная с 2000 года заметно повысился интерес к вопросам расследования преступлений, совершаемых осужденными в местах лишения свободы. Проводятся диссер-

[1] Веб-страница (англ. Web page) — документ или информационный ресурс сети Интернет.

* Под пенитенциарными преступлениями в настоящей статье понимаются преступления, совершаемые осужденными в период отбывания наказания в местах лишения свободы.