УДК 343.985.7; 343.98.067
DOI: 10.17223/22253513/42/5

Е.Р. Россинская, А.И. Семикаленова

ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫЕ КРИМИНАЛИСТИЧЕСКИЕ МОДЕЛИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ КАК ЭЛЕМЕНТЫ КРИМИНАЛИСТИЧЕСКИХ МЕТОДИК (НА ПРИМЕРЕ «КИБЕРШАНТАЖА»)[1]

Новые возможности изучения и обобщения больших массивов криминалистически значимой информации с использованием технологии Big Data позволяют сформировать и реализовать концепцию информационно-компьютерных криминалистических моделей компьютерных преступлений, которые могут служить одним из основных элементов частных криминалистических методик расследования. Использование данного подхода описано на примере расследования «кибершантажа» – вымогательства с использованием сети Интернет.
Ключевые слова: *способы компьютерных преступлений; учение об информационно-компьютерных криминалистических моделях; вымогательство с использованием сети Интернет*

Одним из негативных следствий глобального процесса цифровизации в начале XXI в. явилось возникновение новых видов преступлений, основанных на использовании IT-технологий, причем это не только преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена ст. 28 Уголовного кодекса Российской Федерации (УК РФ), но и широкое применение компьютерных средств и систем для совершения практически любых преступлений: в сфере экономики (кражи, мошенничества, вымогательства), в сфере экономической деятельности, в сфере общественной безопасности и др.

Все эти преступления нами ранее было предложено именовать «компьютерными преступлениями», причем мы неоднократно подчеркивали, что дефиниция «компьютерное преступление» должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом преступления и, соответственно, с методикой его раскрытия и расследования.

Нами разработана научная основа раскрытия и расследования компьютерных преступлений – теория информационно-компьютерного обеспечения криминалистической деятельности, *предметом* которой являются закономерности возникновения, движения, собирания и исследования компью-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003.

терной информации при расследовании преступлений и судебном рассмотрении уголовных дел. *Объектами* теории являются, с одной стороны, сами компьютерные средства и системы как носители розыскной и доказательственной криминалистически значимой информации, а с другой – система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий выявления, фиксации, изъятия, сохранения, исследования и использования криминалистически значимой доказательственной и ориентирующей информации [1]. В систему теории входит ряд учений: о способах компьютерных преступлений / правонарушений [2]; о цифровых следах как источниках криминалистически значимой компьютерной информации [3]; о криминалистическом исследовании компьютерных средств и систем [4].

Очередным этапом нашего исследования является изучение проблемы создания криминалистических методик расследования компьютерных преступлений. Следует отметить, что традиционно одной из главных составляющих любой методики выступает криминалистическая характеристика вида преступления, хотя с этой дефиницией в криминалистической литературе связаны неутихающие дискуссии. Так, профессор Р.С. Белкин указывал, что «криминалистическая характеристика приобретает практическое значение лишь в тех случаях, когда между ее составляющими установлены корреляционные связи и зависимости, носящие закономерный характер». А том виде, как она излагается в учебниках криминалистики, она носит ходульный характер: «легче описывать элементы характеристики, да еще по собственной схеме, чем заниматься весьма трудоемким процессом выявления корреляционных зависимостей между ними» [5. С. 220–224]. Профессора В.Я. Колдин и Е.П. Ищенко предлагали замену криминалистической характеристики типовой информационной моделью преступления, которая позволяет на основе выявленных статистических зависимостей между ее элементами получать новый источник актуальной криминалистически значимой информации [6].

Не вдаваясь более подробно в дискуссию, отметим, что в основе дефиниции криминалистической характеристики преступлений, отстаиваемой множеством авторов, или часто противопоставляемой ей типовой информационной модели лежит, по нашему мнению, необходимость моделирования данного вида преступления путем обобщения на основе изучения больших массивов уголовных дел сведений о криминалистически значимых признаках вида преступления и их закономерных связях между собой.

За последние 20 лет IT-технологии сильно продвинулись, активно идет процесс цифровизации уголовного судопроизводства [7], что обусловило реальную возможность обобщения больших массивов информации. В этой связи большой интерес представляет позиция А.А. Бессонова, который выступил с предложением о формировании цифровых криминалистических моделей преступлений, когда с учетом подхода к криминалистической характеристике вида преступления как к информационной модели

возможно «создавать цифровые модели, максимально адаптированные к использованию в цифровой среде… по сути, речь идет о цифровизации типовых криминалистических характеристик преступлений, т.е. о представлении их в форме соответствующих цифровых моделей» [8].

Однако для компьютерных преступлений следует учитывать, что одним и тем же способом могут совершаться различные виды преступлений: например, путем анонимизации своих действий в сети Интернет построением цепочки прокси-серверов. Так, технологии VPN обеспечивают шифрование сетевого трафика между компьютером пользователя и VPN-прокси-сервером, который является шлюзом выхода в сеть Интернет и, соответственно, скрывает реальный IP-адрес пользователя. Если им требуется высокий уровень конспирации, преступники арендуют у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, на которых настраивают собственные VPN-серверы либо виртуальные машины.

Способы компьютерных преступлений являются полноструктурными, поэтому могут быть выбраны различные способы подготовки, совершения и сокрытия, слабо коррелирующие с видом преступления. Так, большинство троянских программ сочетает целый набор функций, предоставляющий преступникам самые широкие возможности для манипулирования пользовательской информацией. Например, Trojan-Banker.Win32.RTM, помимо присущей только этому виду троянских программ функциональности поиска и копирования пользовательской информации, обладает возможностями поиска файлов по именам, записи истории нажатий клавиш клавиатуры, записи видео и создания снимков экрана, копирования буфера обмена, блокирования и нарушения работы операционной системы, получения от сервера управления команд на запуск дополнительных программных модулей, отправки собранной информации на сервер управления и т.п. Поэтому традиционное объединение информационных моделей по видам преступлений не дает необходимых результатов. Еще в конце прошлого века, когда IT-технологии только начинали использоваться в преступной деятельности, мы предлагали для компьютерных преступлений понятие родовой криминалистической характеристики ввиду общности способов этих преступлений [9], которая предполагает общность способов преступлений в пределах данного криминалистического рода.

Общность способов для различных видов преступлений, совершаемых с использованием IT-технологий, обусловливает формирование типовых информационно-компьютерных моделей преступлений нового типа, которые будут отличаться предметами посягательства, в какой-то степени потерпевшей стороной, но характеристика лиц, совершающих преступления, связана в первую очередь с их уровнем владения компьютерными технологиями.

Полагаем, что в рамках теории информационно-компьютерного обеспечения криминалистической деятельности, с опорой на учения о способах компьютерных преступлений, о цифровых следах как источниках крими-

налистически значимой компьютерной информации, о криминалистическом исследовании компьютерных средств, актуально формирование основ нового учения об информационно-компьютерных криминалистических моделях компьютерных преступлений. *Предмет* этого учения составляют общие закономерности построения информационно-компьютерных моделей компьютерных преступлений на основе корреляционных связей комбинаций IT-технологий и компьютерных систем для осуществления различных способов компьютерных преступлений независимо от их вида, со следовой картиной в виде цифровых следов и с компетенциями в информационных компьютерных технологиях преступника и потерпевшей стороны. *Объектом* учения является криминалистически значимая компьютерная информация об использованных комбинациях IT-технологий и компьютерных средств и систем для осуществления различных компьютерных преступлений, о цифровых следах, в том числе следах воздействия вредоносных программ, о контрафактных информационно-компьютерных продуктах, а также характеристика лиц, совершающих данные преступления, с точки зрения степени владения ими информационными компьютерными технологиями.

Основным принципом формирования информационно-компьютерных моделей является ранжирование их по сложности способов реализации противоправных действий, включая используемые IT-технологии и корреляции с этими способами уровня компетенции преступников, состава преступной группы или сообщества. Корреляционные связи существуют также между способом компьютерного преступления и компьютерной грамотностью потерпевшего, которая также может иметь разные уровни компетентности. Информационно-компьютерные модели компьютерных преступлений при обобщении больших массивов информации могут служить одним из основных элементов частных криминалистических методик расследования.

Рассмотрим использование данного подхода на примере расследования одного из быстро распространяющихся и постоянно модифицирующихся видов преступлений – вымогательства с использованием сети Интернет, или, как его еще называют в литературе, «кибершантажа» [10. С. 288]. Эта проблема имеет транснациональный характер, и ей уделяется достаточно большое внимание в зарубежной литературе, где данное явление приобрело наименование ransomware [10–17]. Однако следует подчеркнуть, что данный вопрос в основном рассматривается с точки зрения обеспечения информационной безопасности (Information Security). В криминалистическом же аспекте данная проблема пока мало разработана, что не может не вызывать сожаления, поскольку «кибершантаж» сегодня набирает обороты, его жертвами становятся не только физические, но и юридические лица. По данным Лаборатории Касперского, 3 596 вредоносных пакетов оказались мобильными троянцами-вымогателями только в первом квартале 2021 г. [18]. Нижняя граница суммарного ущерба от действий программ-вымогателей, по оценкам Group-IB, составляет более 1 млрд долл. США [19].

«Кибершантаж» – это противоправное действие, которое охватывает диспозиции сразу нескольких статей УК РФ (ст.ст.163, 137, 183, 272, 273 и др.). Основным объектом данного преступления / правонарушения являются имущественные права физических и / или юридических лиц. Однако по совокупности правонарушений дополнительным объектом будут неприкосновенность тайны личной жизни, коммерческой, банковской и налоговой тайны, общественные отношения по безопасному использованию компьютерных средств и сетей. Расследование данных видов преступлений представляет сложность в основном из-за использования в процессе их совершения компьютерных средств и сетей, что влечет за собой большие проблемы в установлении места совершения преступления и лица, его совершившего. С позиций учения об информационно-компьютерных криминалистических моделях компьютерных преступлений рассмотрим способы данных преступлений, характеристики лиц, их совершающих, и лиц, оказавшихся потерпевшими, прежде всего отмечая их компетенции в IT-технологиях.

Начнем с рассмотрения преступлений в отношении физических лиц. Наиболее распространенной задачей преступников является получение информации о частной жизни путем внедрения в компьютерные средства и средства связи потерпевшего программного обеспечения, позволяющего: осуществлять запись, блокирование или перенаправление звонков, осуществляемых по средствам телефонии видеоконференций связи, мессенджеров; производить запись видео- и аудио- информации, используя внутренние средства компьютерного устройства; копировать данные из адресной книги телефона, почтовых программ и программ обмена сообщениями (мессенджеров); отправлять данные о местоположении; копировать данные; отправлять и получать SMS; отключать антивирусное программное обеспечение; просматривать историю браузера и выполнять иные функции [20. С. 155]. Получив сведения, компрометирующие потерпевшего или его близких, либо иные сведения, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, вымогатели предъявляют требования передачи им чужого имущества, чаще всего денежных средств, путем перевода на указанные счета или путем отправления платных SMS-сообщений. В последнее время получило распространение требование перевода на указанные электронные кошельки криптовалюты различных систем.

Говоря о характеристике потерпевшего, необходимо отметить, что под ударом в данном случае находятся все пользователи сети Интернет. Однако наибольшую опасность такого рода преступления представляют для лиц с невысоким уровнем компетенции в IT-технологиях либо склонных скачивать контент в обход официального производителя, а также увлекающихся компьютерными играми, поскольку именно при обновлениях подобного программного обеспечения, покупке дополнительных функций, зачастую нелегальной, часто и происходит «заражение» компьютерного средства. Именно при распространении условно бесплатного программного обеспечения (ПО) имеются широкие возможности вписать в распро-

страняемый функционал необъявленную функцию, тем самым получив несанкционированный доступ к компьютерному средству. При поиске путей проникновения нелегального программного обеспечения на компьютерное средство необходимо анализировать пути скачивания обновлений, получения дополнительных функций и сами скаченные модули. Представляется достаточно продуктивным производство судебных компьютерно-технических экспертиз этих компонентов с целью установления в них функционального содержания.

Изучение личности злоумышленника, совершающего вымогательство в отношении физических лиц с помощью угроз распространения порочащих потерпевшего или близких ему людей сведений, можно сказать, это лица преимущественно мужского пола в возрасте от 18 до 30 лет, обладающие достаточно высоким уровнем компетенций в области компьютерных технологий. Но необходимо отметить, что постоянно возрастает доля женщин, вовлеченных в данный вид преступлений. Наши исследования показали, что в современных условиях нельзя акцентировать внимание только на лицах, хорошо владеющих IT-технологиями и навыками программирования, поскольку рынок программных продуктов очень широк, и сегодня производители вирусных программ и «троянов» предлагают разнообразное программное обеспечение, а покупателю такого продукта достаточно быть хорошим пользователем, способным самостоятельно разобраться в его применении. Хотя, конечно, это не отменяет необходимости компетенций преступника в основах и принципах функционирования компьютерных средств и сети Интернет.

Другим способом осуществления компьютерного вымогательства является распространение программ-вымогателей, работающих по принципу «троянского коня». Они выполняют втайне от законного пользователя незапланированные им функции: блокирование, изменение или уничтожение информации, нарушение работы компьютеров или компьютерных сетей. Наиболее распространенным является шифрование такими программами областей носителя информации, содержащих пользовательские данные: текстовые, графические, видео- и аудиофайлы, файлы баз данных. Целью действий этих программ является блокирование доступа пользователя к данным на компьютере или ограничение возможностей работы на компьютере и требование денежных средств за возврат к исходному состоянию системы.

До недавнего времени подобного рода атаки совершались в основном на физических лиц, ярким примером может служить вредоносная программа, содержащая сообщение и изображение активиста Anonymous в маске и надпись: «You have been Hacked» («Вас взломали»), текст на фарси с требованием оплаты выкупа в обмен на восстановление закодированных файлов. Мерой успешной борьбы с ней была предупредительная работа с пользователем, который просто мог игнорировать подобное предложение и не кликать на экране кнопку Click Me («Нажми на меня») [21]. Теперь уровень компьютерной компетенции преступников вырос во много раз, а во всем мире потерпевшей стороной уже являются юридические ли-

ца: фирмы, крупные корпорации и даже муниципальные информационные структуры [13, 16, 19, 20, 22]. Если ранее такие программы чаще всего вносили изменения в загрузочные модули программ, операционной системы и т.д., то сегодня это уже шифрование данных. Если ранее специалисты по информационной безопасности организаций могли самостоятельно с использованием данных, полученных от организаций, специализирующихся на написании антивирусных программ [18], провести восстановление системы, то теперь в арсенал преступников вошли алгоритмы шифрования. Для декодирования информации, обработанной ими, требуется знание и этих алгоритмов, и ключей к ним. Так, недавно вымогатели начали использовать сложную гибридную комбинацию симметричного и асимметричного шифрования для кодирования файлов пользователей [15], подобрать ключ к которой практически невозможно. Изменился при данном способе вымогательства не только метод совершения преступления, но и метод передачи имущественных прав. Сегодня это практически всегда выражается в переводах на электронные счета кибервалюты.

Если говорить о потерпевшей стороне в преступлениях, совершаемых с использованием программ-вымогателей, то здесь следует отметить, что характеристика этих лиц претерпела существенные изменения. Конец 2019 г. и весь 2020 г. захлестнула волна программ-шифровальщиков, большинство вымогателей сфокусировались на атаках компаний коммерческого и государственного секторов. Всего за последний год публично известно о более чем 500 атаках [19], т.е. практически имеет место «война», которую развернули специалисты в области защиты информации и преступники-вымогатели. С обеих сторон фигуранты представлены специалистам высокого класса, обладающими знаниями не только в области программирования и других IT-технологий, но и высшей математики и криптографии, что возможно только при наличии высшего образования не ниже уровня бакалавра. Соответственно, возраст таких преступников будет находиться в диапазоне 25–45 лет. При этом отмечается, что процент женщин – участниц данного вида преступления – имеет тенденцию к росту, что, на наш взгляд, объясняется популярностью образования в сфере IT-технологий.

Анализируя следы, возникающие в результате проведения такого рода атак вымогателей, на наш взгляд, необходимо искать не только следы непосредственно «троянских» программ-шифровальщиков, но и следы «программ-разведчиков», собирающих информацию о составе сетевой инфраструктуры предприятия и о его «чувствительных местах», и проводить анализ логов[1] с учетом этих условий.

Следующим способом осуществления кибервымогательства является организация распределенных сетевых атак (DDoS[2]-атак), направленных на

[1] Логи – это файлы, содержащие системную информацию о работе сервера или любой другой программы, в которые вносятся определённые действия пользователя или программы.

[2] Distributed Denial of Service (англ.) – распределенный отказ в обслуживании.

блокирование доступа к сетевым ресурсам потерпевшего внешними пользователями. DDoS-атака – это действия злоумышленников, направленные на нарушение работоспособности инфраструктуры компании и клиентских сервисов. Злоумышленники искусственно создают лавинообразный рост запросов к онлайн-ресурсу, чтобы увеличить нагрузку на него и вывести его из строя [23]. В основе таких атак лежит технологическое ограничение пропускной способности сетевой инфраструктуры, поддерживающей Интернет или телефонные ресурсы потерпевшего. Для DDoS-атаки используют так называемые «ботнет-сети» – компьютерные сети с запущенными на устройствах ботами[1], которые управляются злоумышленниками удаленно. Киберпреступники активизируют запросы с помощью этих ботов, которые обращаются к сайту выбранной жертвы. Боднет-сети могут состоять как из зараженных устройств пользователей (например, компьютеров с активированными на них вирусами, которые хакеры используют без ведома пользователя), так и, например, из IoT-устройств: «умных» колонок, пылесосов и т.д. [Там же]. Размер ботнета может составлять от десятков до сотен тысяч устройств. Во время таких атак в адрес сетевого ресурса отправляется большое количество запросов с целью исчерпать его возможности обработки данных и нарушить нормальное функционирование. Если число запросов превышает предельные возможности хотя бы одного компонента сетевой инфраструктуры, могут возникнуть значительные задержки при формировании ответа на запросы либо полный отказ в обслуживании запроса [20. С. 155]. При подобного рода атаках требования вымогателей всегда связаны с условиями прекращения DDoS-атаки и восстановления работоспособности сетевой инфраструктуры потерпевшего.

Потерпевшей стороной при осуществлении DDoS-атаки являются фирмы, обладающие сетевыми ресурсами, чье взаимодействие с пользователями и потребителями происходит через веб-ресурсы. К ним можно отнести организации, занимающиеся электронной коммерцией, работающие в финансовом секторе, осуществляющие госуслуги, телекоммуникационные услуги, онлайн-обучение, сервисы доставки, социальные сети, мессенджеры, видеоконференцсвязь. Отметим, что ввиду особенностей инфраструктуры подобный род атак вымогателей не осуществляется на физических лиц.

Исследование современной литературы в области анализа личности кибервымогателей [24] и практики производства судебных компьютерно-технических экспертиз позволяет сделать вывод, что сегодня нельзя говорить о совершении компьютерного преступления, квалифицируемого по ст. 163 УК РФ, лицом единолично. Мы имеем дело с повторяющимися, детально подготовленными преступлениями со сложным, многоступенчатым механизмом, основанным на полноструктурном способе преступления, когда сокрытие зачастую происходит одновременно или даже ранее

[1] Бот – автономная компьютерная программа, выполняющая определенные функции. Чаще всего под словом «бот» понимается интернет-бот – автономная программа, работающая через Всемирную сеть.

приготовления к преступлению. Такие деяния могут осуществляться только организованными преступными группами, включающими организатора преступной группы, специалистов в области IT-технологий и программирования, лиц, обладающих компетенциями в области компьютерных технологий и обеспечивающих распространение вредоносных программ, их эксплуатацию с целью последующего перевода кибервалюты в денежные средства и перевод этих средств на подконтрольные счета, лиц, осуществляющих снятие наличных денежных средств со счетов или в банкоматах.

В заключение отметим, что указанные способы, особенно осуществляемые организованными преступными группами, могут быть применены для совершения целого ряда иных компьютерных преступлений. «Кибершантаж» выбран для примера и в силу его распространенности. Учение об информационно-компьютерных криминалистических моделях компьютерных преступлений дает эффективный инструмент при работе с большими массивами уголовных дел (Big Data) при сборе информации и выявлении корреляционных связей способов компьютерных преступлений с компетенциями в области компьютерных технологий и других областей знания преступников и потерпевших. Таким образом, информационно-компьютерные криминалистические модели компьютерных преступлений могут служить основой при построении частных криминалистических методик раскрытия и расследования.

Литература

1. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (99). С. 193–202.

2. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3(148). С. 87–99.

3. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы междунар. науч.-практ. конф. (19 февраля 2019 г.). Алма-Ата : Акад. МВД Казахстана, 2019. С. 6–8.

4. Россинская Е.Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11, вып. 3. С. 745–759.

5. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М. : Норма : Инфра-М, 2001. 240 с.

6. Колдин В.Я., Ищенко Е.П. Типовая информационная модель преступления как основа методики расследования // Известия высших учебных заведений. Правоведение. 2006. № 6 (269). С. 128–144.

7. Вилкова Т.Ю., Масленникова Л.Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу // Вестник Пермского университета. Юридические науки. 2019. № 46. С. 728–751.

8. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 58–61.

9. Россинская Е.Р. Методика расследования преступлений в сфере движения компьютерной информации // Криминалистика. Методика расследования преступлений

новых видов, совершаемых организованными преступными сообществами. М. : Моск. ин-т МВД РФ, 1999. С. 256–271.

10. Лопатина Т.М. Кибершантаж как средство условно-цифрового вымогательства // Вопросы правоведения. 2014. № 4 (26). С. 288–298.

11. Reshmi T.R. Information security breaches due to ransomware attacks : a systematic literature review // International Journal of Information Management Data Insights. 2021. Vol. 1, is. 2. Art. 100013.

12. Faghihi F., Zulkernine M. RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware // Computer Networks. 2021. Vol. 191 (3). Art. 108011.

13. Marett K., Nabors M. Local learning from municipal ransomware attacks: a geographically weighted analysis // Information & Management. 2021. Vol. 58, is. 7. Art. 103482.

14. Lock M. Five steps to beating ransomware's five-minute warning // Computer Fraud & Security. 2020. Is. 11. DOI: 10.1016/S1361-3723(20)30117-2

15. Davies S.R., Macfarlane R., Buchanan W.J. Evaluation of live forensic techniques in ransomware attack mitigation // Digital Investigation. 2020. Vol. 33. DOI: 10.1016/j.fsidi.2020.300979

16. Humayun M., Zaman N., Alsayat A., Ponnusamy V. Internet of things and ransomware: Evolution, mitigation and prevention ‖ Egyptian Informatics Journal. 2020. Vol. 22, is. 1. DOI: 10.1016/j.eij.2020.05.003

17. van Beek H.M.A., van den Bos J., Ugen M. Digital forensics as a service: Stepping up the game // Digital Investigation. 2020. Vol. 35. DOI: 10.1016/j.fsidi.2020.301021

18. Чебышев В. Развитие информационных угроз в первом квартале 2021 года. Мобильная статистика. URL: https://securelist.ru/it-threat-evolution-q1-2021-mobile-statistics/101595/ (дата обращения: 01.06.2021).

19. В Group-IB рассказали об ущербе от атак вирусов-шифровальщиков // ТАСС. URL: https://tass.ru/ekonomika/10092623 (дата обращения: 01.06.2021).

20. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учеб. пособие : в 2 ч. / А.В. Аносов и др. М. : Акад. управления МВД России, 2019. Ч. 1. 208 с.

21. Щеглов В.Ю., Надькина А.А. Угрозы информационной безопасности предприятий в связи с цифровой трансформацией экономики и возможности их нейтрализации // Известия вузов. Поволжский регион. Экономические науки. 2019. № 1 (9). С. 33–39.

22. Hofmann T. How organizations can ethically negotiate ransomware payments // Network Security. 2020. Vol. 2020, is. 10. P. 13–17.

23. Что такое DDoS-атаки и как от них защищаться бизнесу // РБК. URL: https://trends.rbc.ru/trends/industry/6062ec9e9a79477e19624d6a (дата обращения: 01.06.2021).

24. Осипенко А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 181–188.

Rossinskaya Elena R., Semikalenova Anastasia I., Moscow State Law University named after O.E. Kutafin (MSLA) (Moscow, Russian Federation)

INFORMATION-COMPUTER FORENSIC MODELS OF COMPUTER CRIMES AS THE ELEMENTS OF FORENSIC TECHNIQUES (USING THE EXAMPLE OF “CYBER BLACKMAIL”)

Keywords: methods of computer crimes, the doctrine on information and computer forensic models, extortion using the Internet.

DOI: 10.17223/22253513/42/5

Traditionally, one of the key components of any methodology is the forensic character of the type of crime, often considered as a typical information model. The basis of this definition

is, in our opinion, the need to model this type of crime by generalizing based on the study of large arrays of criminal cases, information about the criminally significant signs of the type of crime, and their natural connections. In the era of digitalization, new opportunities are opening up for the study and generalization of large arrays of forensically significant information using BigData technology. The use of information computer technologies in criminal activities makes it possible to commit different crimes (crimes against the person in economics, economic activities, public security and others) using the same methods. Therefore, the traditional unification of information models by types of crimes does not give necessary results. The article deals with the problems of formation and application of the foundations of a new doctrine of information-computer forensic models of computer crimes as part of the theory of information and computer support of the forensic activity.

The subject of this teaching is the general laws for building information-computer models of computer crimes based on correlation ties. These are the ties of combinations of IT technologies and computer systems for implementing various methods of computer crimes, regardless of their type, with a traced picture as digital traces and with competencies in information computer technologies of the criminal and the injured party. The object of the study is forensically significant computer information about the used combinations of IT technologies and computer tools and systems.

This is information about various methods of computer crimes, digital traces, including traces of the impact of ransomware, counterfeit information and computer products, characteristics of criminals and victims from the point of view of the degree of their proficiency in IT technologies. Information-computer models of computer crimes in the generalization of large arrays of information can serve as one of the key elements of private forensic methods of investigation.

This approach is considered on the example of the investigation of extortion using the Internet – "cyber blackmail". Options of "cyber blackmail" of individuals and organizations are considered and information and computer models are built for them. The authors determine the features of correlation of methods of crimes, the used computer tools and systems, objects of encroachment with the competencies of criminals (organized criminal groups) and victims in IT technologies.

References

1. Rossinskaya, E.R. (2019) Theory of information and computer support of criminalistic activity: concept, system, basic patterns. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia*. 2(99). pp. 193–202. (In Russian). DOI: 10.24411/2312-3184-2019-00019

2. Rossinskaya, E.R. & Ryadovskiy, I.A. (2019) Modern means of committing computer crimes and patterns of their execution. *Lex Russica*. 3(148). pp. 87–99. (In Russian). DOI: 10.17803/1729-5920.2019.148.3.087-099

3. Rossinskaya, E.R. & Ryadovskiy, I.A. (2019) Kontseptsiya tsifrovykh sledov v kriminalistike [The concept of digital traces in criminalistics]. *Aubakirovskie chteniya* [The Aubakirov Readings]. Proc. of the International Conference. 19 February, 2019. Alma-Ata: Ministry of Internal Affairs of Kazakhstan. pp. 6–8.

4. Rossinskaya, E.R. & Semikalenova, A.I. (2020) The Fundamental doctrine of the criminalistics study of computer tools and systems as part of the theory of information and computer support for criminalistics activities. *Vestnik Sankt-Peterburgskogo universiteta. Pravo – Vestnik of Saint Petersburg University. Law*. 11(3). pp. 745–759. (In Russian). DOI: 10.21638/spbu14.2020.315

5. Belkin, R.S. (2001) *Kriminalistika: problemy segodnyashnego dnya. Zlobodnevnye voprosy rossiyskoy kriminalistiki* [Criminalistics: problems of today. Topical issues of Russian criminalistics]. Moscow: Norma; Infra-M.

6. Koldin, V.Ya. & Ishchenko, E.P. (2006) Tipovaya informatsionnaya model' prestupleniya kak osnova metodiki rassledovaniya [A typical information model of a crime as a basis for the investigation methodology]. *Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie – Proceedings of Higher Educational Institutions. Pravovedenie*. 6(269). pp. 128–144.

7. Vilkova, T.Yu. & Maslennikova, L.N. (2019) Legitimacy and unification in criminal proceedings: from procedural document forms to the electronic criminal case. *Vestnik Permskogo universiteta. Yuridicheskie nauki – Perm University Herald. Jurifical Sciences*. 46. pp. 728–751. (In Russian). DOI: 10.17072/1995-4190-2019-46-728-751

8. Bessonov, A.A. (2020) Digital forensic crime model as a basis for countering cyber-crime. *Akademicheskaya mysl' – Academic Thought*. 4(13). pp. 58–61. (In Russian).

9. Rossinskaya, E.R. (1999) Metodika rassledovaniya prestupleniy v sfere dvizheniya kom-p'yuternoy informatsii [Methods of investigating crimes in the sphere of computer information movement]. In: Rossinskaya, E.R. et al. *Kriminalistika. Metodika rassledovaniya prestupleniy novykh vidov, sovershaemykh organizovannymi prestupnymi soobshchestvami* [Criminalistics. Methods for investigating new types of crimes committed by organized criminal communities]. Moscow: Moscow Institute of the Ministry of Internal Affairs of the Russian Federation. pp. 256–271.

10. Lopatina, T.M. (2014) Kibershantazh kak sredstvo uslovno-tsifrovogo vymogatel'stva [Cyber blackmail as a means of conditionally digital extortion]. *Voprosy pravovedeniya*. 4(26). pp. 288–298.

11. Reshmi, T.R. (2021) Information security breaches due to ransomware attacks : a systematic literature review. *International Journal of Information Management Data Insights*. 1(2). Art. 100013. DOI: 10.1016/j.jjimei.2021.100013

12. Faghihi, F. & Zulkernine, M. (2021) RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. *Computer Networks*. 191(3). Art. 108011.

13. Marett, K. & Nabors, M. (2021) Local learning from municipal ransomware attacks: a geo-graphically weighted analysis. *Information & Management*. 58(7). Art. 103482. DOI: 10.1016/j.im.2021.103482

14. Lock, M. (2020) Five steps to beating ransomware's five-minute warning. *Computer Fraud & Security*. 11. DOI: 10.1016/S1361-3723(20)30117-2

15. Davies, S.R., Macfarlane, R. & Buchanan, W.J. (2020) Evaluation of live forensic techniques in ransomware attack mitigation. *Digital Investigation*. 33. DOI: 10.1016/j.fsidi.2020.300979

16. Humayun, M., Zaman, N., Alsayat, A. & Ponnusamy, V. (2020) Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*. 22(1). DOI: 10.1016/j.eij.2020.05.003

17. van Beek, H.M.A., van den, Bos J. & Ugen, M. (2020) Digital forensics as a service: Stepping up the game. *Digital Investigation*. 35. DOI: 10.1016/j.fsidi.2020.301021

18. Chebyshev, V. (2021) *Razvitie informatsionnykh ugroz v pervom kvartale 2021 goda. Mobil'naya statistika* [Chebyshev V. Development of information threats in the first quarter of 2021. Mobile statistics]. [Online] Available from: https://securelist.ru/it-threat-evolution-q1-2021-mobile-statistics/101595/ (Accessed: 1st June 2021).

19. TASS. (2020) *V Group-IB rasskazali ob ushcherbe ot atak virusov-shifroval'shchikov* [Group-IB spoke about the damage caused by encryption virus attacks]. [Online] Available from: https://tass.ru/ekonomika/10092623 (Accessed: 1st June 2021).

20. Anosov, A.V. et al. (2019) *Deyatel'nost' organov vnutrennikh del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informatsionnykh, kommunikatsionnykh i vysokikh tekhnologiy* [Activities of internal affairs bodies to combat crimes committed with the use of information, communication and high technologies]. Vol. 1. Moscow: Ministry of Internal Affairs of Russia.

21. Shcheglov, V.Yu. & Nadkina, A.A. (2019) Ugrozy informatsionnoy bezopasnosti predpri-yatiy v svyazi s tsifrovoy transformatsiey ekonomiki i vozmozhnosti ikh neytralizatsii

[Threats to information security of enterprises in connection with the digital transformation of the economy and the possibility of their neutralization]. *Izvestiya vuzov. Povolzhskiy region. Ekonomicheskie nauki*. 1(9). pp. 33–39.

22. Hofmann, T. (2020) How organizations can ethically negotiate ransomware payments. *Network Security*. 2020(10). pp. 13–17. DOI: 10.1016/S1353-4858(20)30118-5

23. RBK. (n.d.) *Chto takoe DDoS-ataki i kak ot nikh zashchishchat'sya biznesu* [What are DDoS attacks and how can businesses defend from them]. [Online] Available from: https://trends. rbc.ru/trends/industry/6062ec9e9a79477e19624d6a (Accessed: 1st June 2021).

24. Osipenko, A.L. (2017) Organizovannaya prestupnaya deyatel'nost' v kiberprostranstve: tendentsii i protivodeystvie [Organized criminal activity in cyberspace: trends and counteraction]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii – Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 4(40). pp. 181–188.