жения целей и решения задач, связанных в уголовном процессе с собиранием доказательств»[1]. При этом, следует заметить, что в уголовном процессе нет таких следственных действий, при производстве которых напрямую, или опосредовано следователь не вторгался бы в сферу охраняемых прав и интересов личности.

Как известно, только в результате осуществления следственных действий, в материалах уголовного дела могут появиться обнаруженные следы, будущие доказательства. Процессуальные пути и средства появления доказательств определены Уголовно-процессуальным законом. Эти пути по своему содержанию различны. Различным является и временной характер с начала проведения следственного действия и до его окончания. Общим для всех следственных действий кроме всего, является и то, что в ходе их производства, следователь не знает, какую роль сыграет тот или иной след, (в широком смысле его понимания) для расследуемого уголовного дела. Вместе с тем, заранее можно сказать, что все следственные действия, их результаты, в большинстве своем будут использоваться в основе производства других следственных действий, укрепляя «фундамент» уголовного дела. Однако назвать эти следственные действия подготовительными, только потому, что они создадут условия для производства последующих следственных действий вряд ли уместно.

Какие же критерии вкладываются в такое деление следственных действий на основные и вспомогательные или подготовительные?

Значимость следственного действия и результатов его производства для уголовного дела зависит от многих факторов, в том числе: от следственной ситуации; наличия (отсутствия), количества и качества другой информации по делу; времени получения доказательственной информации; это прямые доказательства или косвенные и т. д.

Такой же подход относится и к доказательствам. Все доказательства в соответствии с законом равны, чего нельзя сказать о способах их получения. Жесткость применяемого способа получения информации и самих объектов исследования оказывают самое непосредственное влияние на его разрешение к использованию.

Все следственные действия, независимо от их емкости и сложности имеют одни и те же общие предназначения и функции, направленные на получение доказательственной информации — доказательств. Следовательно, и результаты следственных действий включают в себя обязательные последовательные этапы: обнаружение информации, ее предварительное изучение (исследование) и оценку, решение следователя о судьбе обнаруженной информации и ее носителе, игнорирование информации или изъятие ее и приобщение к материалам следственного действия. Этот путь проходит

[1] См. *Вандышев В. В.* Уголовный процесс. Общая и особенная части : учебник для юридических вузов и факультетов. М. : Wolters Kluwer, 2009. С. 162; См.: *Якупов Р. Х.* Уголовный процесс. М., 1999. С. 245.

вся информация, которая по воле следователя обнаруживается и изымается.

В дальнейшем, изъятые следы опять же изучаются и оцениваются следователем на предмет относимости к расследуемому делу. О допустимости не говорится, ибо этот вопрос решается до принятия решения следователя о способе получения информации, воплощенной в результатах материальных и «идеальных» объектов.

При убеждении следователя в том, что изымаемые объекты (информация) относится к расследуемому событию, она подвергается различным методам и приемам исследования, конечный результат таких исследований воплощается и представляется в доказательствах.

Если такое рассуждение (путь) является верным, то все следственные действия и их результаты, составляют звенья одной цепи информации, т. е. цепи доказательств.

Таким образом, все следственные действия работают друг на друга, зависят и дополняют друг друга и делить их на основные, главные и вспомогательные, как это предлагают отдельные ученые, не следует, ибо это может оказать влияние на качество производства отдельных следственных действий и результаты расследования уголовного дела.

М. С. Сергеев[1]

Преступность в сфере информационной безопасности. Актуальные проблемы. Методики их расследования

Параллельно с развитием информационных технологий, электронных платежей развиваются так же и преступное сообщество. По данным Group-IB, объем отечественного рынка киберпреступности за 2012 год составлял — 1,9 млрд долл. Из них 446 млн долларов составляет мошенничество в сфере интернет-банкинга[2]. Злоумышленники на протяжении последних 15 лет традиционно нацелены на банки, так как именно атаки на них, приносят существенную прибыль. Как говорят представители Group-IB: «Значительно проще один раз украсть 100 млн рублей, чем совершить 100 краж по одному миллиону каждая»[3]. На сегодняшний день, банки используют современные способы защиты, к примеру, такие как антифрод-системы, анализирующие платежные поручения, поступающие в

[1] *Максим Сергеевич Сергеев, аспирант Казанского (Приволжского) федерального университета, г. Казань, Россия.*

[2] Оценка объемов рынка киберпреступности в РФ. URL: http://report2013.group-ib.ru/.

[3] Киберпреступность. Красть стали меньше, но все равно очень много. URL: http://www.pcweek.ru/pc/blog/security/5489.php.

банк. Однако, преступное сообщество на шаг впереди, они стараются найти новые способы хищения, уязвимые места в системе защиты, разрабатывают новые технологии. Популярны на сегодняшний день ботнеты для IOS и Android систем, использующиеся для кражи денежных средств посредством SMS-банкинга.

Электронные деньги стало явлением глобальным, только у одной американской компании PayPal пользователей больше чем населения в РФ — 164 млн человек в 190 странах[1]. По данным всемирного банка, размер доходов неподконтрольных государству в развитых странах мира составляет примерно треть ВВП, в России почти половина.

Ущерб причиненный пользователям ежегодно всемирный банк оценивает 100 млрд долларов в год[2]. В марте 2007 г. были украдены файлы с сервера американской компании TJX Companies. Вскрыта персональная информация, банки заявили, что хакеры могли получить доступ к более чем 94 млн пользовательских счетов[3]. В августе 2009 г. американец Альберт Гонсалес обвинен в воровстве данных 130 млн кредитных карт. Жертвы выбирал из списка успешных людей, составленных журналом Forcher 500[4]. Апрель 2011 самая крупная утечка данных, взлом серверов PS, украдены данные 77 миллионов учетных записей и данные по кредитным картам[5].

При расследовании мошенничества в сфере интернет-банкинга, можно выделить ряд основных действия[6]. Во-первых, по результатам криминалистического исследования, необходимо установить наличие следов причастности внутренних сотрудников банка. В дальнейшем выделить панели управления вредоносным программным обеспечением и установить связь с другими инцидентами информационной безопасности. Далее следует установить круг иных лиц, причастных к преступлению, которые могли оказывать содействие исполнителю. Следующим шагом, является установление детальных сведений структуре панели управления вредоносным программным

[1] http://www.bbc.co.uk/russian/business/2013/09/130916_paypal_russian_roubles_start.shtml.

[2] Угрозы современного мира. URL: http://russia2.tv/video/show/brand_id//15131/episode_id/117178/video_id/117178.

[3] В США похищены данные 40 млн банковских карт. РБК. 2013 19 декабря. URL: http://top.rbc.ru/economics/19/12/2013/895846.shtmlx.

[4] Неутомимый Гонсалес // Российская газета. 2009. 19 авг. URL: http://www.rg.ru/2009/08/19/gonsales.html.

[5] Хакеры взломали геймерскую сеть PlayStation Network. В их руки попали конфиденциальные и банковские данные 77 миллионов игроков. Сама сеть и её сайт до сих пор в офлайне // Газета. 2011. 27 апр. URL: http://www.gazeta.ru/business/2011/04/27/3596053.shtml.

[6] Расследование мошенничеств в интернет-банкинге. URL: http://www.group-ib.ru/index.php/investigation/39-link-cheating-dbo.

обеспечением и получение доказательств использовании ее в конкретном преступлению.

Другим способом вредоносной активности на которой зарабатывают злоумышленники, являются снова набирающие популярность DDoS-атаки. DDoS-атака(от англ. Distributed Denial of Service) — распределённая атака типа «отказ в обслуживании», целью которой является создание условий, при которых пользователи не смогут получить доступ к сайту или веб-сервису из-за его перегрузки[1]. Сегодня DDoS-атаки — самый распространенный тип хакинга, и чтобы им воспользоваться, не нужно даже базовых знаний компьютерных технологий: готовые к использованию бот-сети для DDoS-атак продаются на форумах. Для страховых компаний DDoS-атаки — означают простой Интернет-продаж и работы филиалов. Для трейдерских компаний — простой работы биржи. Одной из самых крупнейших DDoS-атак является атака Spamhaus, организованная прошлой зимой, которая стала своего рода бесплатной рекламой для этого вида нелегальных услуг.Атака затронула сети крупнейших провайдеров, которые в отдельные моменты оказывались перегруженными[2]. Злоумышленники на этом примере убедились в эффективности этого вредоносного способа, и по миру прокатилась волна DDoS-атак. При расследовании DDoS атак необходимо провести ряд действий[3]. Во первых необходимо установить IP адреса атакующего ботнета, время атаки, IP адрес ресурса, на который были направлены неправомерные действия. Зафиксировать фрагменты вредоносного сетевого трафика, собрать иные доказательства позволяющие установить бот-сеть, с которой проводилась атака. Оценить территориальность распределенности бот-сети. Найти центры управлении бот-сетью. Установить личность и местонахождение лиц управляющих бот-сетью[4].

По мнению специалистов[5], основная цель преступников сегодня это малый и средний бизнес, а иногда и крупные компании. Привлекательность крупного бизнеса заключается в том, что у таких компаний, помимо денежных средств, можно похитить информацию. В этих случаях злоумышленники действуют в основном при помощи нанятых инсайдеров или бывших сотрудников, которые

[1] URL: https://ddos-guard.net/ru.

[2] Одна из самых больших DDoS-атак в истории. URL: http://habrahabr.ru/post/174483/

[3] DDoS атаки. Технологии. Тенденции. Реагирование и оформление доказательств. URL: http://seclife.ru/article/ddos-ataki-tekhnologii-tendentsii-reagirovanie-i-oformlenie-dokazatelstv.

[4] Расследование DDoS-атак. URL: http://www.group-ib.ru/index.php/rassledovanie/35-link-denialofserviceinvestigation.

[5] «Лаборатория Касперского» о практике расследования киберпреступлений // CNews. 2013. 24 дек. URL: http://safe.cnews.ru/reviews/index.shtml?2013/12/24/554645.