1. Фильтрация информации в национальных масштабах на государственном уровне. Примером такого решения может служить «Великий китайский файрвол», использование которого позволило сократить даже использование анонимной сети Tor.

2. Разработка международных соглашений в сфере распространения информации. Этот метод менее эффективен, поскольку нормы международного права носят необязательный характер. Сложность соблюдения границ в глобальных сетях признается многими странами, что создает предпосылки к распаду интернета на национальные сегменты.

3. Введение ответственности конечных пользователей. Примером может служить законодательство Германии и Франции. В Российской Федерации ответственность пользователя наступает только при совершении уголовного преступления.

4. Пересмотр порядка доступа к ресурсам сети Интернет. Использование систем ограничения и контроля доступа, мониторинга просматриваемой информации.

Разумеется, все эти меры будут непопулярными, однако если в национальные интересы входит развитие информационной политики, то принимаемые ограничения должны реально работать.

УДК 343.985

Ю.Ф. Каменецкий

ПРИМЕНЕНИЕ СЛЕДОВАТЕЛЕМ ЗНАНИЙ О СИСТЕМЕ «КЛИЕНТ-БАНК» В РАССЛЕДОВАНИИ ХИЩЕНИЙ ПУТЕМ ЗЛОУПОТРЕБЛЕНИЯ СЛУЖЕБНЫМИ ПОЛНОМОЧИЯМИ

В последние годы модернизация экономики и развитие финансовой сферы Беларуси потребовали значительного сокращения времени для совершения оборота безналичных расчетов и платежей. С этой целью для дистанционного управления денежными средствами клиента на большинстве предприятий внедрены системы дистанционного банковского обслуживания, использующие в качестве удаленного рабочего места электронные устройства: персональный компьютер, ноутбук, нетбук, планшетный компьютер и т. д. Наибольшее распространение получили система «Клиент-банк» и интернет-банкинг. Поэтому набравшая темпы информатизация общества не только способствовала стремительному росту компьютерных преступлений, но и видоизменила способ совершения значительной части экономических преступлений, в том числе и хищений путем злоупотребления служебными полномочиями.

В свою очередь, с помощью систем дистанционного банковского обслуживания способ совершения хищений путем злоупотребления служебными полномочиями предопределяет специфику следообразования, поскольку действия преступника неизбежно связаны с совершением безналичных расчетов и платежей. В силу сказанного для установления способа совершения преступления, выдвижения версии и отыскания следов хищения огромную роль играет криминалистически значимая информация о первичных учетных документах, отражающих преступные действия и указывающих на лиц, их совершивших. Однако в настоящее время научно обоснованные рекомендации по получению такой информации из системы «Клиент-банк» в ходе расследования хищений путем злоупотребления служебными полномочиями отсутствуют.

Личный опыт автора и анализ судебно-следственной практики указывают, что эффективное расследование таких уголовных дел напрямую зависит от уровня знания следователями порядка функционирования системы «Клиент-банк». Например, с использованием знаний о работе этой системы следствию удалось своевременно получить сведения о способе преступления и собрать достаточные доказательства для привлечения директора предприятия Х. и главного бухгалтера М. к уголовной ответственности по ч. 4 ст. 210 УК. В частности, Х. и М. с целью хищения безосновательно перечислили с предприятия Б. на подконтрольное им предприятие Ф. деньги с назначением платежа «по договору безвозмездного займа». В действительности договор безвозмездного займа не оформлялся и не мог быть оформлен, поскольку данное право отнесено к исключительной компетенции учредительного собрания. С целью сокрытия своих преступных действий от аудиторской проверки М. и Х. внесли заведомо ложные сведения в бухгалтерский учет предприятия, изменив в платежном поручении запись о назначении платежа: «за поставку техники». В ходе предварительного следствия М. и Х. свою причастность к совершению преступления категорически исключали.

Анализ исходной информации о хищении поставил перед следователем ряд задач по сбору доказательств, связанных с отысканием первичного учетного документа, послужившего основанием незаконного платежа, установлением в составе данного платежного документа корректности, целостности и авторства электронной подписи, а также установлению обстоятельств составления поддельного платежного поручения и помещения его в бухгалтерский учет предприятия. В основе решения данных задач лежала организация следователем различных технических мероприятий, направленных на предотвращение сокрытия следов, уничтожение информации. Для этого были задействованы используемые в

банке средства и методы защиты информации, ее хранения в неизменном виде. С помощью специалиста в сфере высоких технологий информация о реквизитах платежного поручения была зафиксирована и осмотрена в базе данных систем дистанционного банковского обслуживания и базе данных автоматизированной банковской системы.

Более того, следователем из банка затребована информация о движении платежного поручения, его авторстве, дате, времени, способе его создания, а также системах обнаружения вторжения и антивирусной защиты и т. п. Установление исходной информации о первичном учетном документе, с помощью которого совершено преступление, позволило выдвинуть версию о способе совершения Х. и М. хищения и собрать неопровержимые доказательства их вины.

Как показывает практика, расследования уголовных дел, способ сокрытия хищения путем злоупотребления служебными полномочиями может включать не только действия по изменению в бухгалтерском учете сведений о назначении платежа, но и осложняться отражением в таком учете ряда вымышленных операций. Выявить данные фиктивные операции в бухгалтерском учете можно путем анализ платежей в системе дистанционного банковского обслуживания и последующего сопоставления результатов такого анализа с данными бухгалтерского учета.

Например, такой анализ платежей в системе «Клиент-банк» послужил отправной точкой в расследовании уголовного дела по ч. 4 ст. 210 УК в отношении бухгалтера П. предприятия М., которая с целью хищения денежных средств предприятия на основании платежных поручений через систему «Клиент-банк» перечислила денежные средства на предприятия А., Б. и В. за продукцию, которой завладела совместно со своим подельником Е. Для сокрытия совершенного преступления в бухгалтерской программе «1С. Бухгалтерия» в карточках счета платежного поручения контрагентов П. указала вместо фактических получателей иные предприятия Г., Д., Е., с которыми предприятием М. ежедневно осуществлялись различные сделки.

Для получения доказательств о способе преступления следователем произведены осмотры систем «Клиент-банк» и «1С. Бухгалтерия», что позволило зафиксировать информацию о содержании внесенных в бухгалтерский учет недостоверных сведений и должностном лице, осуществившем эти преступные действия с целью сокрытия хищения.

Таким образом, успешное расследование данного уголовного дела опиралось на своевременное получение информации о платежах, производстве следственных действий для закрепления следов преступления в системе дистанционного банковского обслуживания, использующего электронные устройства клиента банка.

Подводя итог, следует подчеркнуть, что компьютерные технологии, принятые на вооружение в финансовой сфере страны, значительно видоизменяют способ совершения хищений путем злоупотребления служебных полномочий, а следовательно, и следовой картины в системе «Клиент-банк».

Сегодня отправной точкой в расследовании этих преступлений является уровень знаний следователем возможностей систем дистанционного банковского обслуживания и особенностей отражения в ней следов хищений данного вида. В настоящее время одним из способов улучшения качества и оперативности расследования может стать систематическая работа по повышению профессионального уровня следователей, специализирующихся на расследовании данных хищений.

УДК 343.985

А.Г. Кулага

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Возможности, предоставляемые международным технологическим прогрессом, телекоммуникационными инновационными системами, внедрением компьютерной техники, заключают в себя не только положительное влияние на общество и государство, но и угрозы безопасности.

В процессе обмена информацией, использования инновационного высокотехнологичного оборудования во всех сферах жизнедеятельности государств между пользователями телекоммуникационных платежных международных систем возникает множество различных вопросов в сложившейся ситуации.

Развитие компьютерных технологий, их внедрение в деловую сферу во всех направлениях общественной жизни привело к возникновению преступлений, в результате которых преступники для завладения чужим имуществом используют высокотехнологическое оборудование. Это заставило правоохранительные органы более активно включиться в борьбу с новыми способами хищений с использованием компьютерной техники. В связи с этим при расследовании преступлений против информационной безопасности, хищений с использованием компьютерной техники в даче правовой оценки возникают проблемные вопросы в выявлении преступлений с использованием компьютерной техники, во взаимодействии специалистов правоохранительных органов, в