При кажущейся простоте тезиса, что от человека зависит все, мы должны признать, что многие поведенческие свойства личности зависят от объективных предпосылок, определяющих деятельность субъекта. Теоретический анализ данных предпосылок деятельности субъектов ОРД, на основе современного состояния противодействия преступности, обязывает нас выработать адекватные меры противодействия криминалу. При таких условиях, как: ведомственная разобщенность правоохранительных органов, поиск критериев оценки оперативной работы, наличие проблемных аспектов ведомственного контроля за осуществлением рассматриваемой деятельности, сложностях при участии оперативного сотрудника в выполнении процессуальных функций, осуществляемых им как субъектом органа дознания; наличие проблем в стадии возбуждения уголовного дела, дублирование функций с другими подразделениями ОВД, есть необходимость в формировании целостной, логически завершенной концепции деятельности субъектов ОРД в современных условиях.

УДК 334.722.012.64:004.77:343.72

В. П. Сабадаш
доцент кафедры уголовного права и правосудия
Запорожского национального университета,
кандидат юридических наук, доцент

ОСНОВНЫЕ СПОСОБЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВА В СФЕРЕ ЭЛЕКТРОННОГО БИЗНЕСА

Созданный и активно развивающийся мир компьютерных технологий открыл широкие возможности для человечества. В виртуальном пространстве можно общаться, искать необходимую информацию, обрабатывать ее и использовать, работать и получать за это вознаграждение, совершать покупки в интернет-магазинах, то есть человек может полноценно реализоваться. Однако этот процесс имеет и негативную сторону: увеличение количества преступлений против собственности с использованием компьютерной техники – интернет-мошенничество.

Особенно актуализировался этот вопрос в современном обществе, поскольку в Украине, как и в других странах, значительно выросло количество людей, которые делают покупки в интернет-магазинах, пользуются онлайн банковскими услугами – оплачивают счета, управляют своими банковскими сбережениями и т. д. WorldWideWeb стал областью электронного бизнеса, который быстро разрастается и в котором циркулируют огромные деньги, что делает данную область особо привлекательной

для интернет-мошенников, технически и компьютерно грамотных, имеющих необходимую современную технику.

Надо отметить, что наиболее распространенными в сфере электронного бизнеса являются следующие способы интернет-мошенничества:

1) фишинг и его разновидности – вишинг и смишинг;
2) мошенничество с платежными пластиковыми карточками;
3) мошенничество при пользовании мобильными телефонами, в том числе при осуществлении платежей с помощью premium-SMS.

Фишинг (производное от английского слова fishing – рыбалка) – это вид мошенничества, целью которого является выманивание у доверчивых или невнимательных пользователей сети персональных данных клиентов онлайновых аукционов, сервисов по переводу или обмену валюты, интернет-магазинов. Мошенники используют различные поводы, заставляющие пользователей лично расстаться с конфиденциальными данными – например, направляют электронные письма с предложениями подтвердить регистрацию аккаунта, которые содержат ссылки на сайт, чей дизайн полностью копирует дизайн известных ресурсов.

Целью фишеров сегодня являются клиенты банков и электронных платежных систем. Особенностью деятельности современных фишеров является то, что если раньше мошенники действовали от имени известных банков и компаний, рассылая миллионы писем, например, с темой «Необходимое восстановление учетной записи», которые отправляли наивных пользователей на подставные веб-сайты, то теперь ссылки на фальшивые серверы прячут в середину кода письма, показывая пользователю ссылку в виде действительного адреса. То есть увеличивается количество случаев использования вирусов-червей и шпионских программ для незаметной перенаправки пользователей на фальшивые сайты.

Кроме того, сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые как бы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определенному номеру для решения проблем по их банковским счетам. Эта техника называется «вишинг» (голосовой фишинг). Позвонив по определенному номеру, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счета на PiN-код. Вишеры могут сами позвонить жертвам, называясь представителями официальных организаций, используя фальшивые номера.

Активно набирает обороты и SMS-фишинг, известный как смишинг (англ. SMiShing – от «SMS» и «фишинг»). Мошенники рассылают сообщения, которые содержат ссылки на фишинговый сайт; заходя на сайт, и вводя свои личные данные, жертва аналогичным образом передает их

злоумышленникам. В сообщении также может говориться о необходимости перезвонить по определенному номеру для решения «возникших проблем».

Все большее распространение набирает такой вид преступления, как мошенничество с платежными пластиковыми карточками, который как серьезная проблема возник в 90-е годы XX столетия, и сегодня ежегодные потери от подобных преступлений составляют десятки миллиардов долларов.

Официальная статистика свидетельствует том, что количество преступлений, связанных с использованием пластиковых карт, ежегодно увеличивается в несколько раз, а материальный ущерб увеличивается в арифметической прогрессии по сравнению с хищениями, совершенными традиционным способом.

Подделка кредитных карт, кража при помощи электронно-вычислительных машин стали настоящимо бедствием в США, Италии, и других странах. Компании, особенно банки, пытаются скрыть факты компьютерных краж, поскольку опасаются падения доверия вкладчиков, акционеров, партнеров. Поэтому официальная статистика не отражает фактического состояния данной проблемы. Кроме того, жертвы часто сами не подозревают, что их обокрали. Эксперты считают, что в США при помощи ЭВМ из банков воруют в четыре раза больше, чем при вооруженных ограблениях.

Платежи с помощью premium-SMS в украинском обществе, традиционно относящемся недоверчиво к кредитным картам как к электронным методам оплаты услуг, сегодня становятся не только самым популярным способом платежей, но и самым опасным.

Так, злоумышленники обманывают пользователей, предлагая им скачать контент и указывая цену SMS, которая ниже реальной в 10–15 раз, заражают мобильные телефоны пользователей вирусами, которые со временем сами рассылают сообщения на premium-номера, кодируют файлы, содержащиеся на жестком диске, а иногда блокируют функционал операционных систем, требуя в обмен на лечение отослать SMS на какой-нибудь из premium-номеров.

Другими словами, мошенники постоянно находят новые способы отбирания денег у населения, и у всех этих способов есть как минимум один признак – короткие мобильные номера с очень дорогими SMS.

Стремление сетевых преступников понятно: если при других способах интернет-мошенничества злоумышленнику нужно пройти достаточно долгий путь от момента обмана пользователя до получения живых денег (например, получить данные кредитной карты при помощи поддельного сайта, потратить деньги на товары в интернет-магазинах и только потом превратить товар в деньги, продав вещи по неоправданной

цене), то в случае premium-SMS реальные деньги можно получить буквально через неделю.

Таким образом, на сегодняшний день такой сегмент рынка, как электронная коммерция, все чаще подвергается нападениям интернет-мошенников, которые используют новейшие достижения науки и техники с целью получения преступных доходов. И только знание способов борьбы и профилактики сможет остановить развитие и процветание мошеннических проявлений в интернете.

УДК 343.132:004.9

Т. А. Савчук
доцент кафедры конституционного
и административного права Академии управления
при Президенте Республики Беларусь,
кандидат юридических наук

ЭЛЕКТРОННАЯ ФОРМА УГОЛОВНОГО ДЕЛА КАК ЭЛЕМЕНТ ИНФОРМАТИЗАЦИИ СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ: ПРЕДПОСЫЛКИ И ПРОБЛЕМЫ ВНЕДРЕНИЯ

На современном этапе в Республике Беларусь наблюдается стремительное внедрение информационных и коммуникативных технологий во все области жизнедеятельности, включая сферу уголовной юстиции. Это послужило импульсом для обсуждения в научной литературе различных инициатив по оптимизации нормативной базы и практического применения таких технологий в уголовно-процессуальной деятельности, центральной идеей которых является переход от бумажного документооборота к электронному. Действительно, развитие отечественного законодательства главным образом сдерживается взглядом на письменность как на основную и незаменимую форму фиксации в уголовном процессе. Но в условиях современного состояния развития науки и информационных технологий, активной государственной политики в сфере электронного правительства этот взгляд может быть заменен на отношение к письменности как главной, но не единственной и вполне заменимой форме фиксации информации в уголовном процессе.

В связи с этим отдельные ученые (А.Ф. Абдулвалиев, М.И. Федорова) настаивают на введении в уголовно-процессуальное законодательство норм, предусматривающих новую форму уголовного дела – электронную. В качестве аргументов в ее пользу данные авторы указывают ненадежность бумажного носителя (его ветхость и легкое уничтожение), объемность и тяжеловесность томов уголовного дела, а