летних детей на иждивении у виновного, молодой возраст и состояние здоровья подсудимого, состояние здоровья и возраст его близких родственников.

Зачастую злоумышленники занимают руководящие должности в организациях (главный бухгалтер, генеральный директор), которые впоследствии незаконно создают либо реорганизуют юридическое лицо, так как им известен механизм возможного ухода от ответственности, правила составления учредительных документов и доверительные отношения с территориальными органами налогового контроля.

Судимость как один из признаков группы персонографических обстоятельств имеет значение при установлении лица, совершившего преступление. Судебная практика показывает, что чаще всего в качестве организатора преступления выступают лица, ранее не привлекавшиеся к уголовной ответственности, либо были судимы ранее за преступления в сфере экономики (ст. 159, 172 УК РФ) и судимость была снята в порядке, установленным законом.

Таким образом, типичным преступником совершения анализируемых преступлений является мужчина возрастной группы от 25 до 45 лет, находящийся в браке, получивший высшее образование, связанное с юридической либо экономической специализацией, обладающий способностями грамотно составлять документы отчетности; как правило, судимости не имеет либо был ранее судим за преступление в сфере экономики. Чаще всего субъект преступления действует исходя из целей дальнейшего незаконного обналичивания и транзитирования денежных средств.

В заключение согласимся с мнением Н.В. Полякова о том, что «в настоящий момент в Российской Федерации достаточно широко развита целая индустрия по обналичиванию и транзитированию денежных средств, позволяющая заинтересованным лицам уклониться от уплаты налогов, вывести активы за границу, легализовать денежные средства, полученные преступным путем. Во главе этой незаконной деятельности стоят лица, поставившие осуществление незаконной банковской деятельности на широкий и бесконтрольный поток, что в первую очередь является причиной нахождения страны в состоянии глубокого финансового кризиса. Бороться с данными проявлениями можно только коренными изменениями действующего законодательства и путем тщательной и скоординированной работы правоохранительных органов, что позволит резко сократить число совершаемых экономических преступлений, в т.ч. и по ст. 172 УК РФ»[1].

Алескеров В.И.,

кандидат юридических наук, доцент
Всероссийский институт повышения квалификации МВД России (г. Домодедово)

DOI 10.51980/2021_1_293

Колокольчикова О.Н.

Всероссийский институт повышения квалификации МВД России (г. Домодедово)

Некоторые способы хищения денежных средств в системе дистанционного банковского обслуживания

Предлагаем рассмотреть некоторые способы преступлений, совершаемых в системе дистанционного банковского обслуживания[2]: использование вредоносных программ скрытого управления; использование программ считывания

[1] Поляков Н.В. К вопросу о необходимости совершенствования современного российского законодательства для борьбы с незаконной банковской деятельностью // Алтайский юридический вестник. 2017. № 4 (20). С. 100.

[2] Данный перечень не является исчерпывающим, так как возможно появление новых способов хищений денежных средств, а также в какой-то части измененных.

пароля; применение программ удаленного доступа; создание «зеркального сайта».

Использование вредоносных программ скрытого управления. В данном случае преступниками используется вредоносная программа, которая проникает и устанавливается в мобильный телефон потерпевшего. Далее она самостоятельно (без непосредственных команд преступников) рассылает с него SMS-сообщения, управляя его банковским счетом через услугу «Мобильный банк».

Данная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в SMS- или MMS-сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты.

Одним из признаков (необязательным) наличия вредоносной программы на мобильном телефоне является направление «пустых» SMS или MMS-сообщений на телефоны, имеющиеся в контактах устройства. При открытии адресатом такого SMS или MMS происходит дальнейшее заражение вирусом телефонов, получивших данное сообщение.

Возможно получение потерпевшим в виде SMS с номера 900 или других сервисных номеров различной информации, которую он не запрашивал. Это связано с тем, что направление информации с сервисных номеров вызвано действиями вредоносных программ.

Одним из способов первичного средства выявления вредоносных программ на телефоне является использование антивирусных программ, получение детализации телефонных звонков и SMS. При наличии вредоносной программы в разделе детализации «исходящие SMS» будут сообщения, которые владелец телефона не направлял на сервисный номер 900 либо номера, используемые преступниками для списания средств потерпевшего через поступившие SMS.

Предлагаем рассмотреть некоторые примеры рассматриваемого вида преступлений. Сотрудниками Управления «К» в рамках оперативного сопровождения уголовного дела, возбужденного СЧ ГУ МВД России по СКФО по ч. 2 ст. 273 УК РФ, установлены и задержаны участники организованной преступной группы, действовавшей под руководством жителя г. Владикавказа, который разработал уникальное вредоносное программное обеспечение для хищения конфиденциальной информации и скрытой генерации криптовалюты на «зараженных» технических устройствах.

Следственные действия в отношении участников группы по множеству фактов противоправной деятельности производились одновременно на территории девяти субъектов Российской Федерации.

В результате сопровождения уголовного дела, возбужденного по ч. 4 ст. 159 УК РФ, сотрудниками Управления «К» на территории г. Москвы установлен и задержан злоумышленник, которым разработано уникальное программное обеспечение, позволяющее эксплуатировать уязвимости терминалов системы «UPOS» и получать одобрение платежных операций без подтверждения банком. Указанной уязвимости на текущий момент оказались подвержены более 1,7 млн платежных терминалов ПАО «Сбербанк России».

В ходе раскрытия преступления было установлено, что мошенники расклеивали QR-коды на прокат автомобилей и велосипедов, в местах, где продавцы отсутствовали. Клиент, ничего не подозревая, сканировал QR-код, после чего оплачивал услуги по прокату. Денежные средства поступали напрямую мошенникам на их лицевые счета, а клиент оставался без денежных средств и услуг проката (схема).

Схема. Мошенничество с использованием QR-кода

Использование программ считывания пароля. В этом случае в индивидуальное электронное устройство потерпевшего проникает и устанавливается вредоносная программа, которая фиксирует вводимый пользователем логин и пароль в момент доступа к удаленному банковскому сервису (например, «Сбербанк Онлайн»). Преступники позже, используя этот логин и пароль, входят в личный кабинет пользователя с другого компьютера и совершают хищение.

Применение программ удаленного доступа. Преступниками используется программа, которая предварительно устанавливается на электронное устройство потерпевшего лица. Она позволяет в режиме реального времени отправлять на него команды управления через сеть Интернет (действие аналогично программе «Android» и др.). Отличие от способа, рассмотренного выше, заключается в непосредственном управлении преступниками перечислением похищаемых денежных средств путем удаленного направления команд мобильному устройству (данный способ встречается сравнительно реже иных).

Создание «зеркального» сайта. Данный способ возможен, когда потерпевший пользуется «личным кабинетом» на сайте банка. Преступниками создается и используется фейковый (поддельный) сайт, адрес которого и внешнее оформление страниц трудноотличимы от официального сайта банка, интернет-магазинов, страницы в социальных сетях. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто набирает название банка в поисковой системе, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен вход на «зеркальный» сайт, то вводимыми данными для входа в кабинет банка (логин и пароль) могут воспользоваться злоумышленники и войти на настоящем сайте от имени потерпевшего в его личный кабинет. Далее возможен перевод денег со счета потерпевшего из личного кабинета или подключение к его счету услуги «мобильный банк» на любом абонентском номере.

Основным признаком посещения клиентом «зеркального» сайта банка является то, что после ввода логина и пароля на странице пользователя появляется надпись о техническом обслуживании сайта или любая иная информация. В данном случае информационное SMS-сообщение от банка о входе в личный кабинет может отсутствовать или поступит информация, в которой будет указано: «Обратиться на сайт позднее».

Преступления в сфере компьютерной информации совершаются преимущественно молодыми людьми, ранее не

привлекавшимися к уголовной ответственности. Наибольшую криминальную активность проявляют лица от 14 до 35 лет. Значительная их часть имеет специальное образование, связанное со сферой компьютерных технологий, но встречаются и те, кто получил знания и навыки, способствующие совершению преступлений, самостоятельно.

Преступления в сфере компьютерной информации могут совершаться высококвалифицированными специалистами, владеющимит полной информацией и пониманием принципа работы компьютерных вредоносных программ. Одним из главных признаков преступлений в сфере информационных технологий является то, что совершать преступления могут все лица, вне зависимости от возраста.

Их положение в обществе может варьироваться от школьника и студента до ответственного сотрудника учреждения, компании (фирмы). Отдельные члены преступной группы в некоторых случаях могут проживать в различных регионах и до момента задержания и доставления в органы внутренних дел лично не встречаться с другими соучастниками. Для знакомства и координации своих действий они используют сайты и специальные сетевые ресурсы, где обсуждают способы совершения преступлений и маскировки следов.

Наиболее актуальные вопросы, касающиеся данной проблематики, мы постараемся детализированно рассматривать в своих дальнейших публикациях.

Дубынин Е.А.,

кандидат юридических наук, доцент
судья Уярского районного суда Красноярского края в почетной отставке,
Юридический институт Сибирского федерального университета (г. Красноярск)

Космодемьянская Е.Е.,

кандидат юридических наук, доцент
Сибирский юридический институт МВД России,
Юридический институт Сибирского федерального университета (г. Красноярск)

Проблемные аспекты доказывания виновности лица при расследовании причинения вреда здоровью человека

Жизнь и здоровье человека являются высшей ценностью общества, что непосредственно закреплено в ст. 2 Конституции РФ.

Несмотря на то, что в настоящее время наблюдается некоторое снижение преступлений, связанных с умышленным причинением вреда здоровью человека, все же количество подобных преступлений является значительным. По стране в 2020 г. количество лиц, здоровью которых причинен тяжкий вред, уменьшилось на 3,2% (3150). По сравнению с 2019 г. число лиц, погибших в результате преступных посягательств, сократилось на 1,1% (2350). Красноярский край на протяжении ряда последних лет уверенно находится на 3 месте по количеству совершенных преступлений данной категории[1]. Процент раскрытия преступлений, связанных с причинением вреда здоровью, является высоким в силу их очевидности, вместе с тем и количество оправдательных приговоров достаточно большое и имеет тенденцию к увеличению. Так в 2017 г. были оправданы 47 человек, в 2018 г. – 73, в 2019 г. – 118. Не сокращается и количество прекращенных дел по реабилитирующим основаниям[2].

Рассмотрим некоторые аспекты, связанные с формированием доказательственной базы при расследовании данных преступлений, и ошибками, допускаемыми при производстве отдельных

[1] URL: www.http://crimestat.ru/) (дата обращения: 03.02.2021).
[2] URL: www.http://stat.апи-пресс.рф/stats/ug/t/11/s/1 (дата обращения: 03.02.2021).