# ПРИЗНАКИ РАБОТЫ ВРЕДОНОСНОЙ ПРОГРАММЫ НА МОБИЛЬНОМ ТЕЛЕФОНЕ

*И.М. Проскурин*
Барнаульский юридическийо институт МВД России, г. Барнаул

Современные характеристики преступной деятельности в сфере информационных технологий свидетельствуют о ее качественных изменениях. Прежде всего, это латентные преступления (Т.Н. Богданова в своем труде говорит о сверхвысоком ее уровне [**Ошибка! Источник ссылки не найден.**, с. 65], так же как и В.А. Мазуров [2, с. 153]) либо преступления, квалификация по которым занимает большое количество времени. Механизм совершения хищений денежных средств, с использованием вредоносного программного обеспечения, отличается своей динамичностью, появлением новых способов, связанных с различными ухищрениями, изощренными формами противодействия, что вызывает на практике трудности выявления и документирования указанных преступных действий оперативно-розыскными средствами и методами. Между тем, доказательственная база по такой категории уголовных дел формируется именно на основе результатов оперативно-розыскной деятельности (далее – ОРД). Стремительные темпы развития современных информационных и финансовых технологий позволяют организованной преступности использовать новые платёжные механизмы, как возможность получения преступного дохода.

Характер и способ совершения преступлений в сфере информационных технологий, создание и использование высокоорганизованных схем хищения и вывода денежных средств граждан, связанный с незаконным получением доступа к их конфиденциальной информации, вызывает широкий общественный резонанс. Эффективная организация работы правоохранительных органов по выявлению и раскрытию такого вида преступлений способствует защите материального благополучия граждан России. Так, по данным компании «Лаборатории Касперского» только в первом квартале 2018 года их антивирусным программным обеспечением отражены попытки запуска вредоносного программного обеспечения, предназначенного для кражи денежных средств с использованием мобильных устройств, 1 350 277 пользователей [3]. Причем, в этих цифрах не учитываются распространения вредоносного программного обеспечения для иных компьютерных средств. Вышеизложенное свидетельствует об актуальности разработки современной методики выявления и

раскрытия хищений денежных средств, совершаемых с использованием вредоносных программ на всех его этапах – предварительного расследования и судебного разбирательства.

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» Уголовный кодекс был дополнен статьёй 159.6. В соответствии с новой нормой за хищение чужого имущества или приобретение права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей предусмотрена уголовная ответственность, которая призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей.

Деятельность правоохранительных органов по указанным делам часто не результативна из-за отсутствия знания у оперативных работников методических начал рассмотрения материалов предварительной проверки о хищениях денежных средств, совершаемых с использованием вредоносных программ и имеющихся научно-технических достижений в этой области [4].

При проведении доследственных проверок необходимо наличие проведенного компьютерно-технического исследования, свидетельствующего о работе вредоносного программного обеспечения на мобильном устройстве (сузим оперативно-розыскную ситуацию до случая хищения денежных средств со счета мобильного телефона либо банковской карты, привязанной к мобильному банку абонентского номера сотового оператора с использованием вредоносного программного обеспечения установленного на мобильный телефон потерпевшего) для надлежащей квалификации преступного деяния по ст. 159.6 УК РФ. Учитывая, что сроки проведения исследования колеблются от одного месяца до полугода (в зависимости от загруженности экспертного учреждения) автором предлагаются некоторые признаки, по которым возможно предварительно выявить работу вредоносного программного обеспечения на мобильном устройстве.

Осуществляя разбирательство по фактам хищения денежных средств, совершаемых с использованием вредоносных программ, главной целью является сбор достаточной доказательной базы. Для

этого сотрудники оперативных подразделений должны применять современные методики выявления и документирования, что и обуславливает потребность в научной разработке настоящей темы исследования.

В ходе работы по проверке сообщений о происшествиях, связанных с хищением денежных средств с банковских карт или со счета мобильного телефона с использованием вредоносного программного обеспечения первое, на что следует обратить внимание – операционная система мобильного телефона, находящегося в пользовании у обратившегося гражданина. Наиболее распространенные из них, представленные на российском рынке мобильных устройств:

1. «IOS» (до 24 июня 2010 года — iPhone OS) («АйОс») – операционная система компании «Apple» («Эпл») – имеет закрытый исходный код;
2. «Windows Phone» («Виндовс фон») – имеет закрытый исходный код;
3. «Android»(«Андроид») – операционная система, имеющая открытый исходный код [5].

Доступность исходного кода программного обеспечения делает его привлекательным и более доступным для осуществления манипуляций по дописки вредоносных дополнений и поиску уязвимостей лицами, которые разрабатывают или модернизируют вредоносное программное обеспечение. Исходя из этого, можно сделать вывод о том, что основной вредоносный удар принимают устройства на операционной системе «Андроид», реже на «Windows Phone», крайне редки случаи (в ходе анализа уголовных дел на территории Алтайского края не выявлено ни одного факта) для «iOS» [5].

Второе, на что следует обратить внимание – журнал входящих и исходящих смс-сообщений в телефоне обратившегося гражданина. Если в нем присутствуют смс-сообщения, к которым обратившийся гражданин не имеет отношения – это тоже может свидетельствовать об удаленном управлении телефоном правонарушителем. Однако следует учитывать тот факт, что такого рода сообщения могут скрываться от визуального просмотра пользователем в памяти телефона либо удалятся из памяти телефона вирусной программой поэтому, предлагается сравнение журнала входящих и исходящих смс-сообщений с детализацией по счету абонентского номера сотового телефона. Наличие противоречий между указанными массивами информации является третьим и

наиболее ярким, по мнению автора, признаком работы вредоносного программного обеспечения на мобильном устройстве.

Применение указанной методики поэтапного диагностирования оперативно-розыскной ситуации на практике даже по трем указанным признакам позволит оперативным работникам уже на первоначальном этапе рассмотрения материалов проверки (без наличия проведенного программно-технического исследования) иметь представление о квалификации совершенного деяния по ст. 159.6 УК РФ и проводить первоначальные оперативно-розыскные действия исходя из специфики указанного преступления незамедлительно. Например: изъятие аппарата сотового телефона потерпевшего и направление его на компьютерно-техническое исследование с целью выявления работы на нем вредоносного программного обеспечения, его идентификации и изъятия на носитель информации. На практике действия оперативных работников, не применяющих указанную методику анализа оперативно-розыскной ситуации, приводит к бездумному и поголовному изъятию сотовых телефоном у потерпевших, перегрузке работы экспертных учреждений и неподтверждением первоначальных версий, и, как следствие, потерю драгоценного времени.

**Библиографический список**

1. Богданова Т.Н. Причины и условия совершения преступлений в сфере компьютерной информации // Вестник Челябинского государственного университета. 2013. № 11 (302).Право. Вып. 36. С. 64–67.

2. Мазуров В.А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции // Вестн. Том. гос. ун-та. 2007. №300-1., 151-154.

3. Отчет Лаборатории Касперского «Развитие информационных угроз во втором квартале 2017» // https://securelist.ru/it-threat-evolution-q1-2018-statistics/89767/

4. Поляков В.В., Никитин А.С. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 87-95.

5. Андроид // Википедия. URL: https://ru.wikipedia.org/wiki/Android, (дата обращения: 28.11.2018); Windows Phone // Википедия. URL:, https://ru.wikipedia.org/wiki/Windows_Phone, (дата обращения: 28.11.2018); iOS // Википедия. URL: https://ru.wikipedia.org/wiki/IOS, (дата обращения: 28.11.2018).