

ПРОТИВОДЕЙСТВИЕ ТЕНЕВОМУ ОБОРОТУ МОБИЛЬНЫХ ТЕЛЕФОНОВ УГОЛОВНО-ПРАВОВЫМИ МЕРАМИ



Владислав ШАЛЬКЕВИЧ,
старший прокурор отдела
Генеральной прокуратуры,
юрист 2 класса,
кандидат юридических наук



Александр МАКАРЕВИЧ,
заместитель начальника управления
ГСУ ПР МВД
майор милиции

Проблема хищений мобильных телефонов остро стоит во всем мире. Анализ международного опыта позволяет выделить несколько подходов, применяемых к ее решению: от полного бездействия в урегулировании этого вопроса до применения комплекса организационных, технических и правовых мер, к которым относятся блокирование работы мобильного телефона оператором сотовой связи по IMEI*; уголовное преследование лиц, изменяющих IMEI похищенного телефона с целью недопущения идентификации похищенного оборудования; разъяснение абонентам операторов сотовой связи последствий использования мобильного оборудования с измененными идентификационными данными.

В Сингапуре специальный орган Infocomm Development Authority of Singapore (IDA), регулирующий телекоммуникационный сектор этой страны, не требует от операторов мобильной связи установки оборудования для отслеживания и блокирования похищенных телефонов по IMEI. IDA выразил сомнения в реальной эффективности этого вида систем в контексте рынка мобильной связи в Сингапуре. Свою позицию он обосновал высокой стоимостью эксплуатации систем слежения и блокирования, а также коротким сроком эксплуатации мобильных телефонов. Вместо этого операторам мобильной связи в случае потери или хищения телефона рекомендуется применять приостановку обслуживания абонента и замену SIM-карт [1].

В Великобритании в 2002 году было похищено или утеряно около 700 тысяч телефонов, в 2007 году — более 800 тысяч. Несмотря на критические высказывания представителей

* IMEI (International Mobile Equipment Identity) — международный идентификатор мобильного оборудования (обычно 15-разрядное число в десятичном представлении), уникальный для каждого мобильного телефона GSM- и UMTS-стандарта. Он присваивается при изготовлении и служит для идентификации устройства в сети связи. IMEI хранится в памяти аппарата, как правило, указан на упаковке, в гарантийном талоне, а также под батареей мобильного телефона.

операторов сотовой связи, в эксплуатацию была введена система блокирования работы похищенного оборудования по IMEI [2].

Так как IMEI в похищенном телефоне может быть произвольным образом изменен*, в 2002 году был принят нормативный правовой акт — Mobile Telephones (Re-programming) Act, устанавливающий уголовную ответственность за изменение IMEI без письменного согласия производителя телефона, за обладание средствами, позволяющими изменять IMEI, и др. [3].

В Республике Беларусь в 2007 году совершено 103 082 кражи, из них 21 303, или 20,7 % — хищения мобильных телефонов. За 5 месяцев 2008 года зарегистрировано 6 398 краж мобильных телефонов. В связи с этим Генеральным прокурором поставлена задача разработать действенную систему мер, позволяющую исключить использование украденных сотовых телефонов [4].

Проверкой, проведенной Генеральной прокуратурой, установлено, что только у одного из операторов сотовой связи под одним IMEI используется более **95 тысяч** мобильных телефонов. В то же время на обслуживании данного оператора находится около **270 тысяч** телефонов с измененными идентификационными номерами.

Генеральной прокуратурой предложено Министерству связи и информатизации во избежание предъявления претензий со стороны правоохранительных органов по поводу обслуживания телефонов с измененными идентификационными номерами, и телефонов, находящихся в розыске в связи с совершенными преступлениями, потребовать от операторов сотовой связи создания системы поиска идентификационных номеров такой категории телефонов и автоматического блокирования их работы, а также внести в договоры, заключаемые с абонентами, разъяснения о последствиях использования мобильных телефонов с измененными идентификационными номерами.

На наш взгляд, возможности действующего законодательства в борьбе с теневым оборотом мобильных телефонов используются не в полной мере. Предусмотренная Уголовным кодексом ответственность за некоторые действия в отношении оборудования для мо-

бильной связи (**изменение IMEI, изготовление мульти SIM-карт***) не применяется**. Такие действия не получают должной правовой оценки, что не только создает условия для использования похищенных и утерянных телефонов (перепродажа, получение услуг связи), но и в целом негативно сказывается на эффективности борьбы с этими преступлениями.

Квалификация действий по изменению IMEI

Для правильной уголовно-правовой оценки действий лица, **умышленно изменившего международный идентификатор мобильного оборудования (IMEI)**, необходимо понимать, что собой представляет мобильное оборудование и каковы его роль и место в системе сотовой связи.

Согласно СТБ 1356-2002 “Система сухопутной подвижной цифровой сотовой связи общего пользования GSM 900” система сотовой связи состоит из:

1. Подсистемы коммутации, которая включает:

- центр коммутации подвижных служб, выполняющий функции коммутации вызовов абонентов системы и стационарной сети;
- регистр пользователя — централизованную сетевую базу данных, хранящую информацию обо всех зарегистрированных абонентах сети данного оператора и видах услуг, которые могут быть им оказаны;
- регистр регистрации посетителя — базу данных, хранящую информацию обо всех абонентах, находящихся в данное время в зоне обслуживания центра коммутации подвижных служб;
- центр аутентификации — базу данных, взаимодействующую с регистром пользователя с целью определения подлинности абонента и недопущения несанкционированного использования сети;
- регистр идентификации оборудования — базу данных, содержащую информацию об оборудовании подвижных станций***.

* Мульти SIM-карта — SIM-карта, позволяющая одновременно пользоваться услугами нескольких операторов сотовой связи.

** До настоящего времени в Республике Беларусь ни одно лицо не было привлечено к уголовной ответственности за изменение IMEI. За изготовление мульти SIM-карт к уголовной ответственности привлечены 2 человека.

*** Регистр идентификации оборудования используется для блокировки вызовов, поступающих от похищенных, незаконно используемых или поврежденных подвижных станций.

* Например, программное обеспечение для изменения IMEI телефонов Samsung можно свободно загрузить с www.samsungpro.ru.

2. Подсистемы базовых станций, которая включает:

- контроллер базовых станций;
- базовые станции, состоящие из приемопередающего оборудования и антенных систем. Базовые станции обеспечивают информационный обмен с подвижными станциями.

3. Подвижных станций, которые состоят из абонентского терминала (именуемого в быту как сотовый телефон) и модуля подлинности абонента (SIM).

4. Подсистемы эксплуатации и обслуживания сети GSM, которая, как правило, включает центр эксплуатации и технического обслуживания — компьютерный центр управления функциями эксплуатации и обслуживания центра коммутации подвижных служб.

Исходя из содержания указанного стандарта IMEI идентифицирует конкретный сотовый телефон в системе сотовой связи аналогично тому, как, например, номер кузова автомобиля идентифицирует автомобиль в системе регистрации автотранспортных средств (при указанной аналогии государственный регистрационный номер автотранспортного средства можно сравнить с SIM-картой).

Если обратиться к ГОСТ ИСО/МЭК 2382-1-99 “Информационная технология. Словарь. Часть 1. Основные термины” и Закону Республики Беларусь от 6 сентября 1995 года “Об информатизации”, то **систему сотовой связи можно определить как компьютерную сеть, в которой сотовый телефон является ее узлом или элементом, идентифицируемым по IMEI.**

Из указанного следует, что непосредственно сам сотовый телефон можно рассматривать, по меньшей мере, с двух позиций:

- 1) как узел компьютерной сети, где он выступает в качестве компьютерной системы*;
- 2) как оборудование, включающее в себя машинный носитель информации (МНИ)**, в котором хранится интересующая нас информация (IMEI).

* Компьютерная система — совокупность функционального устройства и программных средств, обеспечивающих обработку данных (ГОСТ ИСО/МЭК 2382-1-99 “Информационная технология. Словарь. Часть 1. Основные термины”).

** Машинный носитель информации — это магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники (ст. 1 Закона Республики Беларусь от 10 января 2000 года “Об электронном документе”).

Из этого можно сделать предварительные выводы:

1) IMEI хранится в цифровом виде на МНИ, являющемся составным элементом сотового телефона;

2) поскольку для изменения IMEI сотовый телефон отключается от компьютерной сети оператора сотовой связи, в целях правильной уголовно-правовой квалификации его следует рассматривать как МНИ, а не как компьютерную систему (в указанной ситуации он не выполняет функции компьютерной системы).

Значит, действия по изменению IMEI можно рассматривать как умышленное изменение информации, хранящейся на МНИ. Однако эти же действия можно определить и как умышленное уничтожение информации, хранящейся на МНИ, потому что при изменении IMEI первоначально составлявшая его совокупность символов уничтожается заменой другими.

По нашему мнению, разграничить изменение и уничтожение информации можно путем установления направленности умысла. Если он направлен в первую очередь на создание новой информации в целях ее использования при безразличном отношении к старой информации (например, изменяются сведения в платежном документе для получения большей суммы денег), то следует полагать, что имела место модификация информации. Если же для лица, изменяющего информацию, вновь созданная информация имеет второстепенное значение, а целью изменения является именно создание факта отсутствия изменяемой информации (как в случае с IMEI), то умысел явно направлен на уничтожение, а не на изменение информации. Эта проблема обусловлена особенностью информации как объекта материального мира.

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах*. Если уничтожению подвергается имущество, то оно как объект материального мира прекращает свое существование, но информация о нем продолжает существовать. Одновременно с этим возникает новая информация — до уничтожения имущества были сведения о его наличии, после уничтожения появляются сведения о его отсутствии, т.е. при уничтожении ка-

* Ст. 1 Закона Республики Беларусь от 6 сентября 1995 года “Об информатизации”.

ких-либо сведений (информации) мы всегда получаем новые сведения, как минимум, об отсутствии уничтоженных. Поэтому для правильной квалификации преступных действий в отношении информации необходимо определить характер и значение изменяемой информации (например, изменилась только часть некоего значимого объема информации либо самостоятельная информационная единица?), а также цель ее изменения.

Таким образом, действия лица, умышленно изменившего IMEI в целях воспрепятствования дальнейшей идентификации сотового телефона, следует квалифицировать по ч. 1 ст. 351 УК как умышленное уничтожение компьютерной информации.

Этой квалификацией можно было бы ограничиться, если бы способ, с помощью которого изменяется IMEI, не был отнесен законодателем к противоправному. Производителями сотовых телефонов не предусмотрено изменение IMEI пользователем, более того, IMEI защищен от изменения. Для обхода разработанной производителями сотовых телефонов системы защиты IMEI и получения доступа к указанной информации используются специальные компьютерные программы, которые позволяют изменить IMEI.

Следовательно, при изменении IMEI осуществляется из корыстной заинтересованности (в целях получения возможности пользоваться телефоном) несанкционированный доступ к информации (сведения об IMEI), хранящейся на МНИ (модуле памяти сотового телефона), сопровождающийся нарушением системы защиты (определенной изготовителем сотового телефона), т.е. действия, предусмотренные ч. 2 ст. 349 УК, а также осуществляется заведомое использование специальной компьютерной программы (позволяющей обойти систему защиты и изменить IMEI) с целью несанкционированного уничтожения хранящейся на указанном машинном носителе рассматриваемой ин-

формации (сведений об IMEI), т.е. действия, предусмотренные ч. 1 ст. 354 УК.

Аналогичным образом квалифицируют действия по изменению IMEI и в Российской Федерации.

**ОБВИНИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ
по обвинению Т. в совершении преступлений,
предусмотренных
ч. 1 ст. 272, ч. 1 ст. 273 УК РФ
(извлечение)**

Т., обладая достаточными знаниями и навыками работы с компьютерной техникой и средствами мобильной связи, являясь частным предпринимателем, в апреле 2003 года открыл центр по ремонту сотовых телефонов "GSM-Сервис". Действуя из корыстной заинтересованности, Т. неоднократно принимал заказы на смену IMEI сотового телефона, содержащегося в памяти сотового телефона и являющегося уникальным параметром, не подлежащим изменению, который позволяет операторам компаний сотовой связи обнаружить и идентифицировать аппарат в случае его утери либо хищения.

Таким образом, Т. своими умышленными действиями совершил неправомерный доступ к охраняемой законом компьютерной информации, то есть информации в электронно-вычислительной машине (ЭВМ), повлекший уничтожение и модификацию информации, то есть совершил преступление, предусмотренное ч. 1 ст. 272 УК РФ.

Он же, имея умысел на изменение IMEI сотового телефона с использованием вредоносных компьютерных программ, полностью осознавая всю противоправность своих незаконных действий, использовал вредоносные компьютерные программы ("Nokia IMEI changer", "NokiaTool v. 3.25"), предназначенные для изменения IMEI в сотовом телефоне "Nokia-3310", содержащиеся на жестком диске компьютера, находящегося по адресу его местожительства, что позволило без уведомления и согласия собственников компьютерной информации изменять и модифицировать IMEI сотового телефона.

Таким образом, Т. своими умышленными действиями совершил использование программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению и модификации информации, то есть совершил преступление, предусмотренное ч. 1 ст. 273 УК РФ [5].

**Квалификация действий по
изготовлению мульти SIM-карт**

Аналогичный подход следует применить и при уголовно-правовой оценке действий по изготовлению мульти SIM-карт.

По своей природе SIM-карта — это специальный тип смарт-карты, архитектура которой включает микропроцессор и память.

Память SIM-карты содержит записанные производителем:

- операционную систему;
- ICCID — уникальный идентификатор интегральной карты, который дублируется на пластиковой подложке;
- **IMSI** — международный идентификатор мобильной станции, который уникально определяет конкретного абонента во всем мире (доступ к нему защищен ПИН-кодом — PIN 1);
- **Ki** — случайно сгенерированное шестнадцатиричное число, доступ к которому заблокирован производителем на аппаратном уровне (т.е. его нельзя прочесть из памяти карты с помощью программных средств). Копию Ki производитель присылает оператору в зашифрованном виде, в каком оно и помещается в базу данных центра аутентификации оператора. Ki защищен производителем, поскольку на его основании вычисляются комбинации чисел, необходимые для регистрации в сети конкретного абонента.

SIM-карта является компьютерной системой, но в данном случае для квалификации изготовления мульти SIM-карты можно пренебречь частью ее свойств и считать SIM-карту машинным носителем информации.

SIM-карта — это собственность оператора сотовой связи, который позволяет абоненту с использованием кодов PIN 1 и PIN 2 производить некоторые манипуляции с определенными данными: телефонной книгой, списком полученных SMS, списком последних набранных номеров, списком фиксированных номеров, списком сервисных номеров абонента. Иные действия с информацией, содержащейся на SIM-карте, абоненту **не разрешены**, и в зависимости от критичности определенной информации она различными способами защищается.

Следовательно, **для изготовления мульти SIM-карты** из корыстной заинтересованности осуществляется несанкционированный доступ к информации (значения IMSI и Ki), хранящейся на МНИ (модуле памяти SIM-карты), сопровождающийся нарушением системы защиты (определенной изготовителем SIM-карты), т.е. действия, предусмотренные ч. 2 ст. 349 УК, а также осуществляется заведомое использование специальной компьютерной программы, позволяющей обойти систему защиты, т.е. действия, предусмотренные ч. 1 ст. 354 УК.

Постановление о привлечении Г. в качестве обвиняемого в совершении преступлений, предусмотренных ч. 2 ст. 349, ст. 352 и ч. 1 ст. 354 УК Республики Беларусь
(извлечение)

... В период с 2003 года по февраль 2007 года Г. с использованием персонального компьютера, прикладных программ, среди которых "Woron Scan", и специально созданного им для совершения преступления радиотехнического устройства, из корыстной заинтересованности, выразившейся в стремлении извлечь из совершаемого преступления для себя выгоду имущественного характера, а также из иной личной заинтересованности, проявившейся в желании получить удобство в пользовании средствами мобильной связи (изготовление мульти SIM-карт), осуществлял несанкционированный доступ к информации, в том числе IMSI (международный идентификатор абонента мобильной связи) и Ki (ключ аутентификации абонента), хранящейся на машинных носителях (модулях подлинности абонентов — SIM-картах операторов сотовой связи), сопровождавшийся нарушением установленной производителем SIM-карт (являющейся его ноу-хау) программной и аппаратной системы защиты указанной информации, повлекший по неосторожности причинение существенного вреда, выразившегося в нарушении конфиденциальности информации SIM-карт, что привело к ее использованию неустановленными лицами.

Если в ходе изготовления мульти SIM-карты информация о принадлежащих абоненту значениях IMSI и Ki копируется в целях дальнейшего использования (**изготовления копии SIM-карты**), то действия квалифицируются и по ст. 352 УК (в Республике Беларусь известны случаи, когда использование копий SIM-карт наносило ущерб до 80 миллионов рублей).

Список цитированных источников

1. <http://www.ida.gov.sg/Policies%20and%20Regulation/20060424165216.aspx>
2. http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/5221326.stm

3. http://www.opsi.gov.uk/Acts/acts2002/ukpga_20020-031_en_1

4. Василевич, Г. Прокурорский надзор должен быть более эффективным / Г. Василевич // Законность и правопорядок. — 2008. — № 2. — С. 9.

5. <http://www.internet-law.ru/forum/index.php?board=9;action=display;threadid=2687#top>