Приведенные данные показывают, что в последние годы происходит снижение раскрытых преступлений, прежде всего по ст. 272 и 273 УК РФ.

Результаты официальной статистики очень часто весьма поверхностно раскрывают истинную ситуацию, сложившуюся по отдельным видам преступлений в Российской Федерации. Это связано прежде всего с огромным количеством показателей, которые остаются за рамками выводимых для всеобщего обозрения чисел.

Попытки интерпретации данной статистики в рамках научных исследований или официальных выступлений не всегда выглядят убедительно.

Например, назначенный в 2011 г. начальником Бюро специальных технических мероприятий МВД России генерал-майор полиции А.Н. Мошков в одном из выступлений заявил, что «снижение количества возбужденных уголовных дел по статьям 272 УК РФ … и 273 УК РФ … связано с уменьшением количества фактов доступа в сеть Интернет под чужими сетевыми реквизитами, так как благодаря усилиям Управления «К» МВД России провайдеры сети Интернет перешли на более взломоустойчивые технологии».

Следует иметь в виду и высокий уровень латентности преступлений в сфере компьютерной информации. Многие исследователи данного вопроса, ссылаясь на разные источники, отмечают, что в России латентность данных преступлений может достигать 90 %, т. е. 9 из 10 подобных преступлений либо не выявляются, либо не регистрируются правоохранительными органами.

Влияющими на статистику факторами могут также быть выявление в ходе расследования совокупности преступлений либо переквалификация преступления на разных этапах производства по делу (в связи с обнаружением новых сведений и фактов совершенного противоправного деяния или с появлением в уголовном законодательстве близких по ряду признаков составов преступлений). Так, с принятием в 2012 г. Федерального закона от 29 ноября 2012 г. № 207-ФЗ в УК РФ появилась новая статья 159.6 «Мошенничество в сфере компьютерной информации», а с 2017 г. отдельному учету стали подлежать преступления, совершенные с использованием компьютерных и телекоммуникационных технологий.

Существенный разброс в показателях регистрации преступлений в сфере компьютерной информации в разных субъектах Российской Федерации может быть связан также с недостаточной профессиональной подготовкой сотрудников, специализирующихся на расследовании данных преступлений, и отсутствием в их распоряжении необходимого методического материала (методик расследования, в том числе алгоритмов конкретных процессуальных, организационных и тактических действий на этапах выявления, регистрации, расследования указанных преступлений).

Несмотря на интенсивное развитие в России и за рубежом разнообразных информационных (компьютерных) технологий и, соответственно, появление новых видов преступлений, связанных с их использованием, необходимые учебные материалы, используемые для подготовки специалистов в области расследования подобных преступлений как в гражданских, так и в ведомственных вузах, часто отсутствуют. Например, в учебнике 2019 г. по криминалистике для бакалавриата под общей редакцией И.В. Александрова (Том 5. Методика расследования преступлений) раздел, посвященный основам методики расследования преступлений в сфере компьютерной информации, занимает 29 страниц; в учебном пособии 2019 г. «Криминалистическая методика» под общей редакцией А.Г. Филиппова данной тематике отведено 20 страниц; во многих учебниках и учебных пособиях по криминалистике, например, в учебном пособии 2019 г. «Криминалистическая методика» для академического бакалавриата под редакцией Л.Я. Драпкина данные вопросы вообще не рассматриваются.

Несомненно, изучение вышеперечисленных проблем, корректировка форм официальной отчетности, контроль за решением актуальных вопросов со стороны вышестоящих органов в расследовании преступлений в сфере компьютерной информации, изменение действующей нормативно-правовой базы, а также разработка необходимого учебно-методического материала позволит повысить эффективность как в борьбе с рассмотренными видами преступности, так и с новыми преступлениями, связанными со сферой информационных технологий.

УДК 004; 343.3/.7

В.Н. Цимбал, кандидат юридических наук,
старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России
sedruk@mail.ru

СОВРЕМЕННЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ВИДЫ, СПОСОБЫ СОВЕРШЕНИЯ И МЕТОДЫ БОРЬБЫ

Согласно статистическим данным ГИАЦ МВД России, за январь–сентябрь 2019 г. зарегистрировано более 205 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных

технологий, что на 69,2 % больше, чем аналогичный период прошлого года.

Почти половина подобных преступлений относится к тяжким и особо тяжким – 99 тыс. Средства, при помощи которых они совершаются: с использованием сети Интернет (108,5 тыс.), средств мобильной связи (78,5 тыс.), компьютерной техники (14 тыс.) и программных средств (4,5 тыс.).

Уголовное законодательство Российской Федерации (РФ) определяет преступления в сфере компьютерной информации в гл. 28, а именно ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», а также помимо вышеобозначенной главы к такого рода преступлениям относится ст. 159.6 «Мошенничество в сфере компьютерной информации».

Конвенция о преступности в сфере компьютерной информации ETS от 23 ноября 2001 г. № 185 предлагает государствам, подписавшим ее, рассматривать несколько групп таких преступлений: против конфиденциальности, целостности и доступности компьютерных данных и систем; связанные с использованием компьютерных средств; связанные с содержанием данных; связанные с нарушением авторского права и смежных прав.

Преступлений в сфере компьютерной информации, согласно указанным статистическим сведениям, за отчетный период всего зарегистрировано 2 577. По отдельным статьям данные следующие: ст. 159.6 УК РФ – зарегистрировано 533 преступления (-29,4 % по сравнению с АППГ), а раскрыто всего 49; ст. 272 УК РФ – зарегистрировано 1 683 преступления (+35,7 % АППГ), а раскрыто всего 343; ст. 273 УК РФ – зарегистрировано 354 преступления (-40,7 % АППГ), а раскрыто больше половины, а именно 185; по ст. 274 УК РФ – сведений нет.

Рассмотрим более подробно обозначенную категорию преступлений, основной отличительной чертой которых является компьютерная информация, под которой в примечании к ст. 272 УК РФ обозначается, что это «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Достаточно большое количество ученых (М.В. Самсонов, О.М. Иванова, С.А. Потапов, Н.А. Каменский, А.И. Халиулин, А.А. Васильев, К.Е. Демин и др.) изучало данное понятие и его значение. Достаточно глубокий анализ провел М.В. Старичков, который пришел к следующему выводу, что «компьютерная информация – это зафиксированные на материальном носителе сведения (сообщения, данные, команды),

представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначены для использования в таких устройствах». С данным мнением, на наш взгляд, стоит согласиться, так как обязательным условием совершения таких противоправных деяний и неотъемлемой его частью являются информационные технологии (компьютеры, средства связи и иное оборудование) и, конечно, информация, обращаемая в них.

Способы совершения компьютерных преступлений различны, выделим следующие:

кража носителя с компьютерной информацией или самого компьютера;

создание программ (компьютерные вирусы, сетевые черви, троянские программы), которые выполняют функции, причиняющие вред компьютерной информации (устройству и/или сети), например, хищение (удаление, модификация) данных, блокирование доступа, удаленное управление операционной системой или сетью, создание бот-сетей, распространение различной информации через зараженный компьютер, шифрование данных и т. п.;

мошеннические действия;

перехват информации;

удаленный несанкционированный доступ;

удаленные (сетевые) атаки: DoS-атаки, анализ трафика, «человек по середине», IP-спуфинг, атаки на уровне приложений и т. д.

комбинированные незаконные действия.

Из вышеуказанного следует, что способов совершения преступлений большое количество, также немало и орудий их реализации. Важными являются методы и применяемые средства для противодействия этим преступным деяниям, проведем некоторые параллели с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Методы борьбы с компьютерными преступлениями можем определить как технические, организационные (в ГОСТе – физический метод защиты), правовые и криптографические. На последнем пункте сильный акцент делать не будем, так как шифрование, как известно, является одним из самых эффективных способов защиты информации, при этом необходимо использовать соответствующее программное обеспечение (например, КриптоПРО) и аппаратные устройства. Применение пользователем криптографической защиты информации не позволит злоумышленнику использовать ее в корыстных и иных целях. Рассмотрим остальные методы подробнее:

1. Технические, т. е. обеспечение защищенности и безопасности компьютера или системы от возможного негативного воздействия при помощи различных программных и программно-технических средств,

а также мер, направленных на обеспечение бесперебойной их работоспособности. Например, использование легального и актуального антивирусного программного обеспечения, шифрование защищаемой информации, применение межсетевых экранов, обновление операционных систем и т. п.;

2. Организационные, т. е. обеспечение физической защищенности информации от ее получения злоумышленниками. Например, постоянное (своевременное, систематическое) обучение обычных пользователей, персонала организаций на предмет информационной безопасности, непренебрежение способами защиты: логины, сложные пароли, иные методы аутентификации, сохранение их в тайне; информирование пользователей о новых видах угроз и способах их реализации; помещение конфиденциальной информации в надежные хранилища и т. д.;

3. Правовые меры, т. е. разработка норм, правил, инструкций, определяющих методы и способы контроля эффективности защиты информации, обозначение ответственности за нарушения. Данная группа относительно эффективна: и уголовное законодательство РФ, и международные документы, и участие РФ в заседаниях международных организаций, которые, в свою очередь, уделяют большое внимание преступлениям в сфере компьютерной информации, киберпреступности и сотрудничеству государств в данной области.

Российской Федерацией признаются существующие проблемы в этой области и ведется следующая работа: в органах исполнительной власти созданы специальные подразделения (например, Управление «К» МВД России, Национальный координационный центр по компьютерным инцидентам, созданный ФСБ России), ведущие борьбу с компьютерными преступлениями; актуализируется законодательство РФ (например, в гл. 28 УК РФ в 2017 г. были внесены изменения, в Доктрине информационной безопасности РФ (указ Президента РФ от 5 декабря 2016 г. № 646) в разд. III компьютерные преступления обозначены как один из видов угроз безопасности страны); подготавливаются кадры для работы в данном направлении (различные учебные заведения); на постоянной основе проводятся дополнительное обучение, переподготовка и повышение квалификации в области информационной безопасности сотрудников различных органов и организаций, а также иная деятельность.

Подводя итог, отметим, что количество совершенных преступлений в сфере компьютерной информации растет, о чем говорят приведенные статистические данные. Происходит это, на наш взгляд, из-за бурного развития информационных технологий, их доступности как для обычного пользователя, так и для преступного элемента. Комплексность подходов по противодействию, борьбе с преступностью и минимизации возможного ущерба от их действий – залог успеха.

УДК 341.23:[343:004.9]

С.А. Чернышева, кандидат технических наук, доцент, профессор кафедры логистики и информационно-математических дисциплин, Минск, БИП – Институт правоведения
s_chernyshova@mail.ru

БОРЬБА С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ – КЛЮЧЕВОЕ ЗВЕНО В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На современном этапе развития информационного общества вопросы информационной безопасности в системе национальной безопасности государства приобретают первостепенное значение и охватывают практически все сферы жизнедеятельности человека.

Компьютерные преступления в контексте информационной безопасности представляют собой противоправные деяния, которые, кроме того, имеют международную природу благодаря устойчивому росту современных средств связи.

В Беларуси количество преступлений в сфере высоких технологий за пять лет стремительно возросло, наметилась устойчивая тенденция к увеличению количества зарегистрированных преступлений в этой сфере.

По данным МВД Республики Беларусь, в 2017 г. было зарегистрировано 3 999 преступлений, в 2018 г. – 4 741, а за 8 месяцев 2019 г. – 5 753 преступления, связанные с IT-технологиями. Такая динамика обусловлена ростом числа зарегистрированных в стране хищений путем использования компьютерной техники и осуществления несанкционированного доступа к компьютерной информации.

В настоящее время борьба с компьютерными преступлениями в сфере высоких технологий требует самого пристального внимания, анализа сложившейся ситуации и принятия конкретных радикальных решений.

Среди мер, направленных на эффективное улучшение ситуации, следует выделить образовательный аспект проблемы, а именно качественную подготовку специалистов нового направления, связанного с обеспечением информационной безопасности.

Так, в Академии МВД Республики Беларусь по инициативе Управления «К» началась подготовка по направлению «Противодействие киберпреступности и компьютерная разведка». Педагоги не только обучают специалистов для Управления «К», но и в целом вооружают сотрудников органов внутренних дел знаниями для борьбы с преступлениями, которые совершаются с помощью информационных техноло-