УДК 343.3

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Франтикова Дарья Александровна,
Карпенко Дарья Сергеевна,
Могилёвский государственный университет имени А.А. Кулешова
(г. Могилёв, Республика Беларусь)

В статье уделено внимание проблеме толкования понятия «компьютерная информация», а также нормам белорусского законодательства, которые направлены на борьбу с преступностью в сфере компьютерной информации и информационной безопасности.

Стоит отметить, что в законодательстве Республики Беларусь не даётся точного определения термину «компьютерная информация», что, в свою очередь, может спровоцировать неверную квалификацию преступных деяний.

По мнению Л.И. Гасан, законодатель традиционно относит к компьютерной информации лишь документированную информацию с определённой структурой, выражаемой в понятной для человека форме, но неопределённой остаётся правовая природа «вторичной» информации, включающей сигналы, команды и данные, образуемые в результате передачи и хранения информации (например, оболочка данных при сохранении информации). Такая информация не обладает признаками документа, но может иметь существенное значение для восстановления информации в будущем. Для устранения указанного пробела следует определить предмет преступления. Компьютерная информация как предмет несанкционированного доступа есть совокупность сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, находящихся в компьютерной системе или на машинных носителях и передаваемых по каналам связи [1].

В нашей стране и за рубежом ежегодно наблюдается рост преступлений против информационной безопасности. Сегодня мы можем говорить о переходе «традиционных» преступлений в виртуальное пространство. Актуальность данного вопроса обусловлена двумя взаимосвязанными явлениями.

Во-первых, повсеместное внедрение высоких технологий в нашу профессиональную и повседневную жизнь закономерно привело к тому, что информационная безопасность стала не просто важным направлением деятельности заинтересованных субъектов, а необходимым условием обеспечения всех сфер

национальной безопасности, политических, экономических, социальных и иных интересов общества и государства. В то время когда у нас принят курс на выстраивание «IT-страны», создание безопасных условий в области информатизации положительно сказывается и на инвестиционной привлекательности государства.

Во-вторых, возможности данных технологий – анонимность, трансграничность, широкий охват аудитории – используются злоумышленниками для совершения весьма обширного круга противоправных деяний: от несанкционированного доступа до незаконного оборота наркотиков и мошенничества.

Киберпреступление – это вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий несанкционированный доступ к компьютерной информации (статья 349 УК Республики Беларусь); модификацию компьютерной информации (статья 350 УК Республики Беларусь); компьютерный саботаж (статья 351 УК Республики Беларусь); неправомерное завладение компьютерной информации (статья 352 УК Республики Беларусь); разработка, использование либо распространение вредоносных программ (статья 354 УК Республики Беларусь). Киберпреступлениями считаются те преступления, в которых ведущую роль играют компьютер или компьютерная сеть [2].

Классифицируя преступления против информационной безопасности, следует подчеркнуть, что:

– цели киберпреступников достигаются путем неправомерного использования информационных коммуникационных технологий, особенно сети Интернет, мобильных средств и систем связи;

– применение информационно-коммуникационных технологий для совершения преступления создает специфические проблемы по установлению правонарушителя, факта и места совершения противоправного деяния, поскольку информационно-коммуникационные ресурсы, используемые для совершения правонарушения, могут находиться одновременно во многих странах;

– доказательства, касающиеся таких преступлений, могут сохраняться и передаваться, как правило, только по электронным сетям (поэтому возникает сложность сбора и закрепления доказательств, проведения процессуальных действий);

– преступления часто совершаются для достижения корыстных целей, однако мотивы преступных деяний могут быть политическими, террористическими и иными;

– возрастает и становится устойчивой тенденция к организованности киберпреступности, усиливающемуся групповому характеру совершения таких деяний, причем объединение злоумышленников часто происходит на добровольной основе.

Рост киберпреступности обусловлен рядом причин: интенсивно идет развитие и популяризация системы безналичных расчетов, появляется все больше устройств, осуществляющих финансовые транзакции. Значительно увеличилось число пользователей всевозможных электронных платежных систем. Наблюдается ежегодный прирост абонентов сотовой связи, держателей банковских платежных карт, интернет-пользователей.

К примеру, по данным МВД Республики Беларусь, в 2018 году зарегистрировано 4741 киберпреступление (это на 53% больше, чем в 2017 году). Большая часть таких преступлений в 2018 году (75,5%) – это хищения путём использования компьютерной техники, 18% – несанкционированный доступ к правовой информации, 3,5% – компьютерный саботаж. Уровень раскрываемости таких преступлений – 53−55%.

Наиболее значительный рост силовики отметили по количеству преступлений, связанных с несанкционированным доступом к информации (статья 349 УК Республики Беларусь), их стало на 97% больше, чем год назад. Основной рост – за счет преступников, которые действуют на профессиональной основе. Можно не обладать большими познаниями в компьютерных технологиях, но иметь представление о природе совершения киберпреступления – основных способах анонимности, разветвленности преступных групп, интернет-сообществах, в которых обсуждают противоправные деяния. Увеличилось число дел, в которых подозреваемые находятся за пределами Беларуси, а потерпевшие – внутри страны. Все это требует адекватной и своевременной реакции как правоприменителей, так и законодателя.

Среди киберпреступников, с которыми сталкиваются белорусские правоохранительные органы, подавляющее большинство – мужчины в возрасте от 18 лет. Одной из основных причин влечения к таким преступлениям является юношеский максимализм и то, что они считают себя «неуловимыми», а также огромную роль играет чувство беззаконности, то есть правовая неграмотность. Рассмотрим самые примитивные и актуальные для молодых людей преступления и варианты наказаний.

Лицом совершён взлом чужого аккаунта в социальных сетях или почте с помощью специальных программ. Часть 1 статьи 349 УК Республики Беларусь – несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда. Наказывается штрафом или арестом.

Лицом совершено изменение личных данных в чужом аккаунте либо ложное размещение информации на сайте. Часть 1 статьи 350 УК Респу-

блики Беларусь – изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации). Наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Лицом совершено изменение пароля чужого аккаунта в социальных сетях, почте, после чего он (пользователь) лишается возможности доступа к своему аккаунту. Часть 1 статьи 351 УК Республики Беларусь – умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж). Наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет [2].

Таким образом, проанализировав XII раздел, главу 31Уголовного кодекса Республики Беларусь (преступления против информационной безопасности), можно отметить, что все преступления в сфере информационной безопасности – умышленные. Несанкционированный доступ к компьютерной информации совершается только по неосторожности пользователей, поэтому для своей же безопасности не следует указывать персональные данные, реквизиты банковских карточек, логины, пароли и иную конфиденциальную информацию в сети Интернет, а также нельзя делиться своими данными с посторонними людьми.

Список источников

1. Гасан, Л. И. К вопросу о трактовке несанкционированного доступа к компьютерной информации (ст. 349 УК Республики Беларусь) / Л. И. Гасан // Правовое обеспечение инновационного развития общества и государства : материалы Междунар. науч. конф. студентов, магистрантов и аспирантов, Минск, 29–30 окт. 2010 г. – Минск, 2011. – С. 229–230.

2. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одоб. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 18 июля 2019 г. № 220-З // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.