вмешательство в данные – противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных (ст. 4);

вмешательство в систему – серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных (ст. 5).

Однако современные преступления в виртуальной сфере стали значительно более разнообразными. Считается, что существует примерно 100 векторов возможных хакерских атак, хотя наиболее известна следующая типизация компьютерных инцидентов:

вредоносное программное обеспечение;

DDoS-атаки;

мошеннические SMS и звонки;

несанкционированный доступ к конфиденциальной информации.

Тремя основными причинами взлома данных являются:

внешняя хакерская атака – 24,6 %;

сбой системы безопасности и внутренние уязвимости – 19,5 %;

человеческий фактор – 18,7 %.

Если вести речь о современных трендах развития преступлений в виртуальной сфере, необходимо отметить, что, согласно докладу о глобальных рисках Всемирного экономического форума, подавляющее большинство экспертов ожидают повышения частоты кибератак, ведущих к краже денег и данных (82 %) и срыву операций (80 %). К 2022 г. к интернету будет подключен один триллион устройств. К 2023 г. у 80 % людей появится аватар в цифровом мире. При этом более 50 % интернет-трафика в 2024 г. будут потреблять «умные» устройства. Ожидается развитие Deepfakes систем для продуцирования правдоподобных сообщений и заявлений, которые смогут воздействовать не только на сознание, но и подсознание людей.

Таким образом, одной из причин ускоренного роста киберпреступности являются технологические тренды. Ожидается использование искусственного интеллекта (ИИ) для борьбы с киберпреступностью. По мере того как организации переходят от центра обработки данных к облачным платформам, использование технологий на основе ИИ будет продолжать расти и получать более широкое распространение. Развитие фейковых видео- и аудироликов, изображений также создает высокий риск быть обманутым. Телефонные боты научатся имитировать знакомый голос человека, который может отдать приказ.

УДК 343.915

В.А. Беспалов

КРИМИНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ЛИЧНОСТИ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЮЩИХ КИБЕРПРЕСТУПЛЕНИЯ

Технологии являются неотъемлемой частью современной жизни человека. Достижения науки и техники открыли множество возможностей для взрослых и детей, улучшая и облегчая жизнь во многих сферах жизнедеятельности. В то же время развитие технологий является не только благом, но и влечет явные угрозы безопасности. Одним из приоритетных направлений государственной политики является обеспечение информационной безопасности, что напрямую связано с использованием информационных технологий. Часто преступления, связанные с использованием компьютерных технологий, совершаются несовершеннолетними.

Таким образом, развитие сферы компьютерных технологий имеет не только положительные, но и негативные последствия, о чем свидетельствует динамика количества преступлений, совершенных несовершеннолетними в сфере киберпреступности. Самым распространенным преступлением, совершаемым несовершеннолетними в данной сфере, является хищение имущества путем модификации компьютерной информации, предусмотренное ст. 212 Уголовного кодекса Республики Беларусь (УК). За период с 2017 по 2021 г. несовершеннолетними совершено 539 таких преступлений. Из них в 2017 г. зарегистрировано 53 преступления, в 2018 г. – 60, в 2019 г. – 144, в 2020 г. – 210, в 2021 г. – 72.

За последние пять лет несовершеннолетними совершено 98 преступлений против компьютерной безопасности, предусмотренных гл. 31 УК. В 2017 г. было зарегистрировано 67 таких преступлений, в 2018 г. – 5, в 2019 г. – 11, в 2020 г. – 12, в 2021 г. – 3.

Несмотря на отсутствие поступательности в динамике киберпреступлений, совершаемых несовершеннолетними, а также на незначительное их количество по отдельным составам в абсолютном выражении, удельный вес таких преступлений в структуре преступности несовершеннолетних остается достаточно высоким.

Субъектом преступлений, предусмотренных гл. 31 УК, может быть вменяемое физическое лицо, достигшее шестнадцатилетнего возраста. За преступление, предусмотренное ст. 212 УК, уголовная ответственность наступает с четырнадцати лет. Такой критерий субъекта, как

возраст, говорит о том, что лицо на момент совершения преступления достигло такого уровня развития, который достаточен для адекватного восприятия характера своих действий и их запрещенности. Как показывает опыт изучения личности несовершеннолетних киберпреступников, субъектом указанных выше преступлений чаще всего являются лица, не имеющие соответствующего образования либо опыта работы в информационной сфере, однако они имеют специальные знания относительно программного обеспечения и владеют некоторыми навыками программирования.

Примечательно, что уровень знаний компьютерных технологий, а также владения компьютерной сетью Интернет отдельными несовершеннолетними уже давно превосходит знания, предусмотренные школьной программой либо программами начальных курсов высших учебных заведений, что позволяет им не только самостоятельно использовать технологии, но и совершать киберпреступления. Таким образом, фундаментом будущей криминальной деятельности является самостоятельное освоение несовершеннолетними информационных технологий.

К наиболее распространенным противоправным действиям несовершеннолетних в сфере киберпреступности относятся следующие: «взлом» страниц в различных социальных сетях; получение незаконного доступа к охраняемой законом информации; совершение кибератак; создание, использование и распространение вредоносных программ; получение несанкционированного доступа к различным игровым ресурсам; осуществление кибертравли; незаконное использование банковских платежных карточек членов семьи или других лиц.

По нашему мнению, можно выделить четыре основные категории несовершеннолетних киберпреступников.

Во-первых, лица, которые, только освоив информационные технологии, хотят проверить свои знания и мастерство или продемонстрировать свои умения. Совершая противоправные поступки, подростки завоевывают внимание сверстников и полагают, что их будут уважать за то, что они умеют это делать. Такие молодые люди обычно совершают преступления, используя несложные методы и примитивные вредоносные программы.

Во-вторых, талантливые молодые люди, которые приобрели достаточно глубокие знания и определенный опыт в области информационных технологий. Они могут создавать довольно опасные компьютерные вирусы, придумывать новые способы заражения компьютеров, а также противодействовать антивирусным программам. Как правило, целью таких преступников является обнаружение инновационных способов проникновения в информационные системы или иных уязвимостей. Они могут не распространять свои программы, но активно продвигают свои

идеи через интернет-ресурсы, посвященные созданию вредоносных программ. Затем такие идеи могут быть использованы другими.

В-третьих, несовершеннолетние, вовлеченные в преступление взрослыми. В таких преступлениях несовершеннолетний может быть как непосредственным исполнителем, так и другим соучастником совершения преступления, например, путем сбора какой-либо информации, разработки вредоносного программного обеспечения или предоставления других средств преступнику.

В-четвертых, лица, чья основная задача – получение незаконной финансовой прибыли. Несовершеннолетние с использованием найденной или украденной банковской платежной карточки, либо с использованием незаконно полученных реквизитов банковской платежной карточки осуществляют снятие денег в банкомате, оплачивают покупки в торговых точках в интернет-магазинах, расплачиваются в онлайн-играх за дополнительные бонусы, уникальные предметы и другие преимущества. Они активируют финансовые услуги, предоставляемые мобильными операторами, на мобильном телефоне другого человека и переводят деньги, предоставленные компанией в качестве займа, на свой абонентский номер телефона.

Несовершеннолетние, являющиеся субъектом того или иного киберпреступления, как правило, не имеют криминального прошлого и часто совершают преступления из-за незнания закона, например, когда подросток не осознает, что «взлом» страницы в социальных сетях или несанкционированный доступ к игровым ресурсам является противоправным деянием и влечет за собой уголовную ответственность.

Таким образом, в связи с тем, что киберпреступления стали совершаться не только людьми, обладающими специальными знаниями в этой области, но и несовершеннолетними, возрастает актуальность борьбы с преступлениями данного вида. Одним из направлений борьбы с преступлениями, совершаемыми несовершеннолетними в сфере киберпреступности, является совершенствование норм УК.

Представляется, что эффективным способом воздействия на несовершеннолетних, совершающих преступления с использованием компьютерных технологий, будет являться закрепление в УК положений, которые позволят ограничивать доступ таких несовершеннолетних к компьютерной технике, определенным информационным порталам и интернет-ресурсам, устанавливать программы дистанционного контроля за телефонными соединениями и интернет-трафиком. Такие положения, по нашему мнению, должны быть включены в п. 4 ч. 1 ст. 117 УК и дополнить перечень форм ограничения свободы досуга несовершеннолетнего.