УДК 343.9.01

Р.А. Белевский

НЕКОТОРЫЕ АСПЕКТЫ И ТЕНДЕНЦИИ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ

Слово «киберпреступление» может быть интерпретировано на основе слова «кибернетика», которое в 1960-е гг. считалось обозначением чего-то передового, связанного с компьютерами, а «кибер» употребляли как приставку к различным словам; с начала 1990-х гг. понятие «кибернетика» метафорично применялось к преступлениям, связанным с компьютерами и интернетом.

Однако в российском правовом (законодательном) поле иностранные метафоры на основе приставки «кибер» не используются.

Хотя Н. Винер считал, что он первым стал употреблять слово «кибернетика», однако этот термин в 1834 г. использовал физик Ампер для обозначения науки об управлении общественными системами, а в 1843 г. польский ученый Ф. Трентовский издал в Познани книгу, которая называлась «Отношение философии к кибернетике как искусству управления народом».

Подчеркнем, что обозначать виртуальный мир как киберпространство нельзя, так как понятие пространства обозначает свойство мира, поля, среды, а не само поле, в том числе и виртуальное. Не надо представлять себе поле как площадку – виртуальное поле может быть многомерным. Если и использовать понятие «пространство», то в значении интернет-пространства (интернет-территории), т. е. как юридический термин, обозначающий наличие национальной юрисдикции на некоторой территории. Однако лучше пользоваться выражением «сфера пространства виртуального мира».

С инфраструктурной точки зрения понятие «интернет-пространство» необходимо рассматривать как глобальное адресное пространство, которое состоит из региональных и (или) национальных сегментов интернета.

Считается, что первое преступление с помощью компьютера в мире было совершено в США в 1960-х гг. Криминологическое определение компьютерного инцидента появилось в 1983 г. Под ним понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных. В СССР первое преступление с помощью ЭВМ «Онега» было совершено программистом в 1979 г. в городе Вильнюсе.

В настоящее время появляются преступники, которые не обладают специальными знаниями, а используют готовые, понятные программ-

ные инструменты. Они, как правило, очень молоды, большинству нет 30 лет. Программы, которыми они пользуются, предельно просты и могут иметь лицензионную политику, а создающие их злоумышленники тратят время на борьбу с пиратством и на защиту своей собственности. Эти сайты предлагают круглосуточную техподдержку на нескольких языках, которой могут позавидовать некоторые производители программного обеспечения.

Словом «хакер» (взломщик) обозначают человека, который способен, используя электронные устройства как инструменты, получить доступ к защищаемым от несанкционированного доступа данным, содержимое которых в виде информации может быть его целью. Поэтому хакеров разделяют:

на «черных» хакеров (хакеров-злоумышленников);

«белых» хакеров, которые проникают в искомую систему без злого умысла;

условных хакеров-программистов, которые должны тестировать систему на предмет выявления в ней уязвимостей.

В определенных случаях программисты могут стать хакерами или, наоборот, хакеры могут работать как условные хакеры. Естественно, все программные инструменты продуцируются самостоятельно программистами и являются нейтральными, но их можно использовать в хакерских целях.

Таким образом, высокотехнологичные преступления в виртуальной сфере подразумевают, что злоумышленники могут пользоваться рынком криминальных программных инструментов. Хакеры объединяются в международные группы и совершают атаки на компьютеры, расположенные в других странах. Поэтому полицейские считают, что для ликвидации незаконных рынков хакерских инструментов, незаконного обналичивания денег требуется объединение усилий полиции для противодействия хакерам из разных государств. Безусловно, необходима Конвенция по борьбе с компьютерными преступлениями на базе ООН, а не только аналогичная конвенция Совета Европы.

Конвенция Совета Европы о киберпреступности выделяет четыре типа компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

незаконный доступ – противоправный умышленный доступ к компьютерной системе либо ее части (ст. 2);

незаконный перехват – противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах (ст. 3);

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