правленности, достаточно велико и их воздействие до конца не изучено. Анализ публикаций показал, что чаще всего в литературе в качестве таких факторов указываются следующие:

– расслоение общества по уровню дохода;

– увеличение безработицы;

– детская и подростковая беспризорность;

– духовно-нравственная трансформация общества;

– миграционные процессы;

– преступления, связанные с наркотиками и незаконным оборотом оружия.

Моделирование – прогнозирование показателей преступности, опирающееся на изучение взаимодействия различных социально-экономических процессов, происходящих в обществе и существенно влияющих на нее.

Поэтому первым этапом построения модели прогноза преступности является выявление факторов, влияющих на количество преступлений террористического характера и экстремистской направленности в наибольшей степени.

Затем с помощью методов регрессионного анализа строится математическая модель, по которой возможно осуществить прогноз количества преступление в будущем. Процесс подбора соответствующей модели распадается на две части: сначала выбирается вид формулы, затем с помощью специальных математических методов подбираются соответствующие коэффициенты, для которых приближение выбранного вида функции к исходным статистическим данным оказывается наилучшим.

Знание причинно-следственных зависимостей между показателями, характеризующими динамику преступлений террористического характера и экстремистской направленности, тенденции ее развития во времени, социально-экономическое состояние рассматриваемой территории, результаты деятельности правоохранительных и других структур, является важным условием противодействия указанным преступлениям и во многом определяет выбор конкретных форм и методов деятельности соответствующих органов.

[1] Состояние преступности в Российской Федерации за январь-декабрь 2017 г. URL: https://media.mvd.ru/files/application/1241295 (дата обращения: 30.01.2018).

[2] Ступина С.А. Современное состояние экстремизма, терроризма и насильственной преступности в Сибирском федеральном округе // Криминологические реалии и перспективы XXI века : материалы Байкальского юридического форума. Иркутск, 2017. С. 86-94.

Комлев Ю.Ю.,

доктор социологических наук, профессор

Казанский юридический институт
МВД России

Киберпреступность в High-Tech эпоху

Технологии меняют жизнь человечества не впервые. В XX веке прогресс информационных технологий привел к «информационном взрыву». Наглядным примером являются данные главы Alphabeth Эрика Шмидта, в соответствии с которыми от начала цивилизации и до 2003 г. было создано около 5 экзабайт (5000000000 Гб) информации. Сегодня же человечество продуцирует такой объем данных всего за 2 дня.[1]

Технологическая революция, информатизация, кибернетизация, интернетизация социума эпохи постмодерна спровоцировали процесс его дальнейшей девиантизации. Инновации, увы, создают не только прогрессивные социальные изменения, порождая новый тип общества, культуры и уровень благосостояния, но и

продуцируют технологически детерминированные формы девиантности и преступности.

Обзор литературы на основе изучения широкого круга зарубежных англоязычных источников и исследований отечественных авторов показал, что к числу совершенно новых исследований нужно отнести работу полицейского аналитика Марка Гудмана (Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It, 2015) и труд отечественных исследователей Е.С. Лариной и В.С. Овчинского[2], а также публикации российских девиантологов Я.И. Гилинского, Я. Костюковского, Ю.Ю. Комлева и других авторов на заданную тему.[3]

В данных тезисах на основе типологизации выделены и структурированы известные и новые виды кибердевиантности.

Основные результаты анализа состоят в следующих обобщениях.

1. Криминализация ряда деяний в России, связанных с правонарушениями в компьютерной сфере, произошла с принятием УК РФ (гл. 28). В 1997 г. были зарегистрированы 33 преступления, а в 2005 г. – 10214, то есть их количество выросло в 310 раз.[4]

2. Понятие «киберпреступность» как разновидность девиантности включает различные формы преступной активности не только в связи с использованием компьютеров или в компьютерной сфере, но и деликты, совершаемые в киберпространстве.

3. Киберпреступность принимает много форм. Она включает: хищение идентификационных данных, интернет-мошенничество, нарушение законов об авторском праве, «взламывание» компьютерных систем, создание и распространение полиморфных вирусов и DDoS-атаки, распространение спама и другие.

4. Современные зарубежные исследователи киберпреступности в рамках интегративного междисциплинарного подхода все больше концентрируются на изучении ряда новых проблем:

– использование инновационных технологий хранения данных в киберпространстве (например, при хищении криптовалюты);

– влияние распространения социальных сетей на киберпреступность;

– использование сетевого фактора в кибертерроризме;

– изучение поведения жертв и преступников в киберпространстве;

– разработка политики и инструментов по обеспечению кибербезопасности;

– защита инфраструктуры от киберпреступности.[5]

5. Незаконный доход среднего киберпреступника в современном Нью-Йорке, по данным полиции, в семь раз превышает добычу обычного преступника. Раскрываемость традиционных преступлений в этом мегаполисе составляет в разные годы от 40 до 60%, а киберпреступлений – 4%. Иными словами, киберпреступность – это высокодоходная и малорискованная криминальная деятельность.[6] Закономерно, что в последние годы при существенном сокращении общего количества преступлений в России криминальная активность постепенно сместилась в виртуальную сферу интернет-пространства.

6. Велик и постоянно растет ущерб от киберпреступлений. В 2018 г. на Всемирном экономическом форуме было признано, что киберпреступность является одним из наиболее критических глобальных рисков.

7. Для защиты глобального киберпространства в Давосе было заявлено о создании Глобального центра кибербезопасности, целью которого является учреждение первой международной платформы для правительств, компаний, специалистов и правоохранительных органов, предназначенной для сотрудничества по преодолению проблем кибербезопасности.

Типологизация киберпреступлений. Анализ зарубежных и отечественных источников позволяет сделать ряд констатаций и обобщений, характеризующих многообразные проявления современной киберпреступности:

1) криминальная активность в интернет-торговле. Проявление данного феномена – явное следствие незаконного дос-

тупа преступников к конфиденциальной информации фармацевтических компаний;

2) киберворовство как похищение программных продуктов. Как свидетельствует отчет компании Software Publishing Association (SPA), глобальные потери от компьютерного пиратства в уже в 1996 г. составили 11,2 млрд. долларов, поскольку на мировом рынке программных продуктов почти каждая вторая разработка является пиратской копией. Некоторые развивающиеся страны имеют особенно высокий уровень незаконного использования программных продуктов. Например, из всех компьютерных программ, используемых во Вьетнаме, 99% скопированы незаконно[7];

3) киберворовство как похищение конфиденциальной информации. Современные киберпреступники могут обнулить банковские счета, стереть содержание компьютерных серверов. До настоящего времени нет компьютерной системы, которую невозможно было бы взломать;

4) киберхулиганство. Уничтожение или изменение приватных или конфиденциальных корпоративных данных с целью компьютерного хулиганства. Создание и распространение разрушительных компьютерных программ-вирусов («червей», макро- или полиморфных вирусов) получило массовое распространение;

5) кибersталкеры. В отечественной литературе, кроме работ Я.И. Гилинского, практически нет упоминаний о новых девиантах кибersталкерах (stalkers – упорные преследователи, «охотники»), в отличие от публикаций зарубежных психиатров и криминологов. Речь идет о девиантах, преследующих кого-либо с использованием различных, в том числе современных технологических средств, прежде всего сети Интернет и сотовой связи. Арсенал современного сталкера включает интернет-ресурсы, телефонные звонки, SMS-сообщения, звонки и сообщения с помощью Skype, обычные и электронные письма, граффити, сообщения в печатных и электронных СМИ. Преследование нарушает частную жизнь жертвы и вызывает у нее непреодолимый страх перед насилием. По данным зарубежных исследователей, жертвами сталкеров являются от 1 до 2% женщин. Физическое насилие происходит приблизительно в каждом третьем случае;

6) новой разновидностью кибersталкерства стал кибербуллинг, обращенный, как правило, к детям и незащищенным социальным группам. Он осуществляется в форме травли, оскорблений или угроз, распространяемых путем рассылки сообщений в социальных сетях, по e-mail или СМС. В детской среде кибербуллинг проявляется в отправке жертве сообщений с угрозами публикации унижающих достоинство жертвы фотографий и видео в социальных сетях или даже в создании поддельных веб-сайтов, нацеленных на унижение и оскорбление жертвы. Информационные технологии позволяют сохранить анонимность кибербуллеру и вытекающую из этого безнаказанность;

7) киберпреступления на транспорте. Специальные программы хакеров могут способствовать краже или поломке автомобиля, поскольку современная машина во многом работает под управлением бортового компьютера;

8) телефонный фрикинг как форма незаконного доступа к сотовому телефону практикуется не один десяток лет. С развитием сотовой связи этот вид девиации получил массовое распространение, включая кражу или нелегальное использование сим-карт сотовых телефонов вызываемых абонентов и кодов доступа с целью обогащения за чужой счет;

9) фрикер-воровство и мошенничество стало острой проблемой в современной России в связи с массовым распространением смартфонов на платформе Андроид;

10) кибермошенничество в банковской сфере. Преступники пользуются тремя основными приемами хищений при использовании интернет-банкинга. Первый способ осуществляется с помощью СМС-банкинга. Второй способ – использование кибермошенниками фишинговых сайтов. В третьем случае фрикеры используют Google Play. Поддельное окно появляется каждый раз, когда держатель мобильного телефона заходит в это популярное приложение и там же он указывает данные своей карты в случае интер-

нет-покупки приглянувшейся программы. Практически во всех указанных случаях киберворы и мошенники остаются безнаказанными.

Таким образом, в эпоху постмодерна, в мире high-tech технологий, носители криминального поведения изощренно используют в своих целях все новые технологические возможности. Современные преступники широко применяют не только огнестрельное оружие, телефон, лекарственные препараты, транспорт, но и компьютеры, сотовую связь, Интернет. Кибердевианты и их незаконная деятельность на основе современных технологий столь же разнообразны, как и сами технологии. Представляется необходимым продолжить девиантологическую дискуссию в заявленном предметном поле и развить исследовательские подходы к изучению новых проявлений киберворовства, киберстокерства и, особенно, кибербуллинга, чреватого серьезными последствиями для здоровья и жизни детей.

[1] Ларина Е.С., Овчинский В.С. Криминал будущего уже здесь («Коллекция Изборского клуба»). М.: Книжный мир, 2017. С. 20.

[2] Там же.

[3] Комлев Ю.Ю. Интегративная криминология: девиантологический очерк. Казань: КЮИ МВД России, 2016; Панфилова Е.И., Попов А.Н. Компьютерные преступления. СПб.,1998; Девиантность в обществе потребления : коллективная монография / под ред. Я.И. Гилинского, Т.В. Шипуновой. СПб.: Алеф-Пресс, 2012.

[4] Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль. 2-е изд. перераб. и доп. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2009. С. 376.

[5] Cybercrime: interdisciplinary approaches to cutting crime and victimisation in cyber space. URL: http://www.newworldencyclopedia.org/entry.

[6] Goodman M. Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It. Doubleday, 2015.

[7] Schmalleger F. Criminology Today: An Integrative Introduction. New Jersey, 1999.

Минисламов М.Н.

Сибирский юридический институт
МВД России (г. Красноярск)

Актуальные проблемы развития киберпреступности: прогнозы и реальность

В настоящее время Указом Президента Российской Федерации в качестве одного из главных направлений обеспечения государственной и общественной безопасности объявлено «совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями» (п. 44 Стратегии национальной безопасности Российской Федерации[1]).

Новые возможности, которые предоставляют информационные технологии, их широкая распространенность и доступность делают эту область чрезвычайно привлекательной для представителей криминальных структур, а динамичное развитие IT-технологий, создание многочисленных информационных ресурсов и баз данных, разработка более совершенных устройств создают условия, облегчающие совершение в этой сфере преступлений, число которых в России с каждым годом увеличивается.

Российское уголовное право оказалось недостаточно готовым к стремительному развитию компьютерной техники и информационных технологий. Всемирная сеть Интернет – весьма удобная площадка для подготовки и осуществления информационно-террористических и информационно-криминальных действий. Так в интернет-пространстве лицами, занимающимися сбытом наркотических средств, могут распространяться реклама магазинов, занимающихся сбытом наркотических средств, рецепты изготовления наркотических и психотропных веществ, информация о трудоустройстве в преступные группы, о местах закладок наркотических средств и способах их оплаты