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

и т.п. Вся эта информация легко маскируется. Отсутствие географических границ, трудно определяемая национальная принадлежность объектов сети, возможность анонимного доступа к ее ресурсам – все это делает уязвимыми системы общественной и личной безопасности.

Результаты социологических опросов, проводимых в России, позволяют охарактеризовать активность общества в виртуальном пространстве как рискогенное, сопряженное с наличием ряда опасностей и угроз. Следует отметить, что интернет-среда продуцирует опасные для психического здоровья, репутации и материального благосостояния общества негативные явления. Среди опрошенных присутствует доля тех, кто имеет некоторое представление об опасности попадания под чужое влияние в социальных сетях, а также часть респондентов полагают, что некоторые информационные ресурсы формируют нужное владельцам этого ресурса общественное мнение, поведенческие установки, мировоззрение. Это относится, по мнению опрошенных, к Facebook (43,2% респондентов), Yandex (34,3%), Google (31,4%), Telegram (28,4%). Как известно, опасность превращается в реальную угрозу, если человек и общество не могут противостоять ей.[2]

За последние пять лет число преступлений, совершаемых с использованием сети Интернет и телекоммуникационных устройств, увеличилось с 11 до 66 тысяч. В 2017 г. наблюдался значительный рост киберпреступлений: их число достигло 40 тысяч. В список основных источников кибератак в России по-прежнему входят собственные сотрудники (77%), криминальные синдикаты (54%), а также хакеры-одиночки (37%). По данным отчета Group-IB «Hi-techcrimetrends» за 2016 г., мнение российских респондентов относительно источников кибератак коррелирует с мнением респондентов по всему миру.

В России две трети преступлений экстремистской направленности и каждое девятое преступление террористического характера совершены с использованием сети Интернет, а также значительное число киберпреступлений связаны с оборотом наркотических средств. Генеральный прокурор Российской Федерации Юрий Чайка отметил, что в России на одном из первых мест среди совершаемых преступлений стоит незаконный оборот наркотических средств, представляющий повышенную опасность для общества. Распространители наркотиков все чаще переходят на бесконтактный способ их сбыта, следовательно, киберпреступность в экономической и социальной сфере будет расти.

С января по сентябрь 2017 г. зарегистрированы 1551,6 тыс. преступлений, из которых 158,5 тыс. связаны с незаконным оборотом наркотиков, что на 3,3% выше показателей аналогичного периода прошлого года. При этом на 6,8% возросло число преступлений, совершенных с целью сбыта наркотических средств, психотропных веществ или их аналогов, а также увеличился их удельный вес в числе преступлений, связанных с незаконным оборотом наркотиков, с 48,8% в январе – сентябре 2016 г. до 50,4% за аналогичный период 2017 г.[3]

На пленарной сессии «Киберпреступность – одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?» в г. Сочи были озвучены следующие прогнозы: количество киберпреступлений в России в 2018 г. может вырасти примерно в четыре раза, а общие потери страны от них могут превысить 2 триллиона рублей. По словам модератора сессии зампреда Сбербанка Станислава Кузнецова, в России сейчас бум диджитализации, и, как следствие, Россия находится в числе главных целей киберпреступников.[4] Чтобы защититься от хакеров, в экономически развитых странах резко увеличиваются затраты на кибербезопасность, а в настоящее время в России даже нет ответственности за фишинг и спам, а максимальное наказание, которое предусмотрено действующим законодательством, не превышает семи лет лишения свободы и штраф в 500 тысяч рублей. В США, например, за эти правонарушения можно получить до 25 лет лишения свободы.

В ходе дискуссий и обсуждений представителями власти и силовых структур были предложены меры, которые, по их мнению, необходимо предпринять для изменения ситуации. В первую очередь,

необходимо определить, кто станет координировать такую работу со стороны федеральных структур и кредитных организаций. Следует также усилить законодательную базу, организовать подготовку специалистов в данной области, на телевидении и других СМИ рассказывать гражданам о существующей опасности (то есть развивать «киберкультуру»), усилить государственное регулирование в этой области для организаций, которые занимаются финансовыми операциями.

Динамика диджитализации и технологической цифровой революции такова, что темпы совершенствования законодательства должны быть принципиально иными. В законодательной базе должна быть предусмотрена ответственность за преступления в сфере информационных технологий, уточнены полномочия органов власти, для того чтобы каждый гражданин понимал, куда обращаться и как наиболее эффективно добиться расследования киберпреступлений и преследования злоумышленников. Если не решать эти вопросы, последствия нашей цифровизации негативно скажутся на экономике России. По данным IXX международного исследования в области информационной безопасности за 2016-2017 годы «Путь к киберустойчивости: прогноз, защита, реагирование», было принято решение о необходимости вести соответствующую работу, и в ближайшее время должен появиться целый ряд законодательных инициатив, которые позволят усилить борьбу с киберпреступностью.[5]

Современное развитие IT-технологий характеризуется непрерывным ростом преступлений и других общественно опасных деяний посредством Всемирной сети, что подтверждено официальной статистикой и научными исследованиями как в России, так и за рубежом. Учитывая эту негативную тенденцию в области правовой борьбы с преступностью в сети Интернет, необходимы решительные меры по противодействию и профилактике данного вида преступлений криминологического и уголовно-правового характера.

Как верно заметил Н.В. Поляков: «При возбуждении уголовных дело незаконном сбыте наркотических средств следователь должен тщательно изучить и проанализировать все материалы доследственной проверки с целью определения механизма совершения преступления, а также последующего планирования следственных действий с привлечением сотрудников оперативных подразделений».[6]

Активное совершенствование алгоритмов поиска информации в ходе проведения оперативно-розыскных мероприятий и следственных действий, тесное взаимодействие с интернет-провайдерами, использование возможностей информационных ресурсов и различных баз данных позволит виновных привлечь к ответственности.[7]

Таким образом, проблема преступности в глобальной сети Интернет является одной из главных составляющих информационной безопасности Российской Федерации, относится к актуальным, своевременным, имеющим теоретическое и практическое значение.

---

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 31.12.2015 № 683 (ред. от 31.12.2015).

[2] Кибакин М.В., Разов П.В. Студенческая молодежь в виртуальном пространстве: опасности и риски // Дайджест научной жизни Финуниверситета. 2017. № 3. С. 27-29.

[3] Данные официального сайта МВД России. URL: https://мвд.рф (дата обращения: 01.11.2017).

[4] Гайфутдинов Р.Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. 2017. Т. 7. № 4А. С. 245-256.

[5] Интернет-портал Минкомсвязь России. URL: http://www.minsvyaz.ru (lata доступа: 30.10.2017).

[6] Поляков Н.В. О необходимости разработки методики расследования незаконной банковской деятельности // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XX международной научно-практической конференции. Красноярск: СибЮИ МВД России, 2017. Ч. 2. С. 262-264.

[7] Минисламов М.Н. К вопросу об участии специалиста при производстве обыска при расследовании преступлений, связанных с незаконным оборотом наркотических средств // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XX международной научно-практической конференции. Красноярск: СибЮИ МВД России, 2017. Ч. 2. С. 252-254.