вания работы над созданием и внедрением новых цифровых форм социального контроля и слежения за пользователями «мировой паутины», участниками сетевого общения. Однако цифровой мониторинг и другие практические аспекты совершенствования социального контроля в цифровом мире все еще недостаточно отрефлексированы в работах интернет-исследователей. Это удел новых, молодых сил в девиантологии и юриспруденции.

Тетерятников Н.Ю.,

кандидат юридических наук
Сибирский юридический институт МВД России (г. Красноярск)

«Виртуализация» преступности: киберугрозы современности

С первых лет третьего тысячелетия в России, как, впрочем, и во всем мире, наблюдается значительное (более чем на 70%)[1] уменьшение количества преступлений. Особенно насильственных. Это явление получило название великого спада преступности – great crime drop.

Причины столь резкого снижения преступной активности до конца так и не ясны. Один из факторов, который, безусловно, этому способствует, – увеличение времени, которое люди тратят на пребывание в информационных телекоммуникационных системах. Начиная от нахождения в социальных сетях, и до часов, ежедневно проводимых за компьютерными играми. То есть, заменяя действительность реальную на виртуальную, у человека элементарно остается меньше времени на то, чтобы совершать в повседневной жизни что бы то ни было, включая противоправные поступки.

Вместе с тем, в пику изложенному необходимо отметить, что, как указывают А. Кнорре и В. Кудрявцев, упомянутое «великое снижение преступности не затронуло две сферы: кражи мобильных телефонов и так называемые e-crimes – киберпреступления, связанные с компьютерами и компьютерными сетями»[2].

Несложно догадаться, что мобильные телефоны пользуются такой популярностью у преступников, поскольку на них наибольший общественный спрос как на самое распространенное в настоящее время средство доступа людей к телекоммуникационным системам, к той самой виртуальной реальности. Что касается киберпреступности, то это ничто иное как побочный, но в какой-то степени и закономерный эффект компьютеризации (а теперь еще и цифровизации) весьма значимой части жизни современного общества.

И если удешевление стоимости мобильных телефонов – это вопрос времени, что в перспективе неминуемо приведет и к снижению соответствующих краж, то сокращения уровня киберпреступности прогнозировать не приходится. Тем более что в настоящее время киберпреступность с постоянно увеличивающимся объемом причиняемого ущерба – это теневая многомиллиардная высокотехнологическая сфера, от противоправной деятельности авторов которой страдают и целые государства, и крупнейшие транснациональные корпорации, и отдельные учреждения, и обычные люди.

В связи с этим целесообразно рассмотреть основные виды киберугроз, с которыми все чаще и чаще приходится сталкиваться нашим современникам.

Одной из самых первых в истории человечества киберугроз, возникшей в 1980-х гг., стали компьютерные вирусы. Это специально созданные вредоносные программы, повреждающие либо уничтожающие пользовательскую информацию, а также препятствующие нормальной работе компьютерной техники.

Изначально большинство компьютерных вирусов не были предназначены для

[1] Великое снижение преступности // Ведомости : электронное периодическое издание. URL: https://www.vedomosti.ru/opinion/articles/2017/09/28/735650-velikoe-snizhenie (дата обращения: 25.01.2020).
[2] Там же.

материального обогащения их создателей или распространителей. Сейчас же вирусы используются преимущественно для создания технических затруднений и сбоев в деятельности конкурентов либо для целей промышленного и иного (коммерческого, политического) шпионажа – по возможности тайного сбора информации, предоставляющей какие-либо преимущества ее обладателям и не находящейся в свободном доступе.

Особой разновидностью вирусов можно считать программы-вымогатели, которые блокируют компьютер пользователя и требуют перечисления денежных средств на определенный счет за разблокировку. Из них наибольшую опасность представляют программы-шифровальщики, которые перекодируют пользовательскую информацию, шифруют ее и не позволяют восстановить данные, пока затребованные денежные средства не будут переведены. Самостоятельные попытки решить проблему могут настолько усугубить ситуацию, что даже перечисление требуемой суммы не поможет восстановить доступ к зашифрованным данным.

Самыми известными программами-шифровальщиками стали компьютерные вирусы «Petya» и «WannaCry», которые в 2017 г. поразили наибольшее количество электронных устройств за всю историю интернета. Начиная с 2018 г. и по настоящее время, активность подобных вирусов по разным причинам (от повышения компьютерной грамотности пользователей до массового использования встроенных в пользовательское программное обеспечение антивирусов) спала[1].

Следующей по распространенности киберугрозой является несанкционированная утечка данных через информационные телекоммуникационные системы. Это становится возможным в результате безалаберности самих пользователей, которые не удосуживаются придумывать изощренные пароли доступа к своим данным, либо вследствие использования разработчиками бэкдор-алгоритмов – программ, встраиваемых в официально распространяемый продукт для негласного получения пользовательской информации или удаленного управления операционной системой пользователя или даже компьютером целиком.

Одним из самых распространенных в России проявлений киберпреступности является фишинг – кибермошенничество, суть которого в получении путем обмана под надуманными предлогами от пользователей денежных переводов или персональных данных, включая номера банковских карт и другой информации, в том числе втайне от самих пользователей. Нередко мошенники звонят или пишут посредством смс либо электронной почты клиентам коммерческих организаций от имени менеджеров с просьбами подтвердить какую-либо информацию, назвав пин-код карты, пароль и прочее. В других случаях используются так называемые «фишинговые письма» якобы от операторов связи, банков или иных контрагентов клиента, активация ссылок в которых приводит к тому, что злоумышленники получают тайный и несанкционированный доступ к данным, содержащимся на компьютере адресата.

Так, в 2019 г. работник сайта bodybuilding.com, доверившись информации, содержащейся в «фишинговом письме», невольно предоставил доступ к клиентской базе данных, в которой были полные имена, адреса места жительства, номера телефонов, адреса электронной почты и другая значимая информация[2].

В качестве пограничного с шантажом и террором вида компьютерных правонарушений можно отметить и так называемый «блекмэйл» – электронные анонимные письма, содержащие угрозу обнародовать компрометирующую адресата информацию, если не будут выполнены требования шантажистов, либо содержащие неподтвержденные (зачастую заведомо ложные) сведения о готовящемся теракте, заложенном в каком-либо учреждении взрывном устройстве и тому подобное.

Ранее злоумышленники для этих целей преимущественно использовали телефонную связь, а сами такие преступления

[1] URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf (дата обращения: 25.01.2020).

[2] Dodybuilding.com discloses security breach. URL: https://www.zdnet.com/article/bodybuilding-com-discloses-security-breach/ (дата обращения: 25.01.2020).

получили обобщенное наименование телефонного терроризма. Однако при использовании телефона необходимо было делать в каждое учреждение отдельный звонок, была вероятность идентификации звонящего с помощью фоноскопического сравнительного исследования. Теперь же с переходом от телефонных сетей на связь посредством интернета особенность этого вида киберпреступлений состоит в том, что современные электронные почтовые сервисы позволяют удаленно (например, из-за границы) создавать анонимные аккаунты для рассылки, в том числе массовой, каких угодно сообщений на любые адреса.

Так, в ноябре 2019 г. – январе 2020 г. по российским городам от Мурманска до Хабаровска прокатилась волна ложных сообщений на адреса электронной почты госучреждений, судов, школ, больниц, почтамтов, станций метро, авто- и ж/д вокзалов, аэропортов, храмов, торговых центров и гостиниц об их минировании с целью сорвать нормальную работу. Поскольку согласно требованиям гражданской обороны при поступлении подобной информации проводится полная эвакуация, пребывают саперы, иные специалисты, и пока они все не проверят и не подтвердят безопасность объекта, вернуться к его эксплуатации нельзя.

По оценкам Интерфакса, только в Москве общее число эвакуированных за это время составило более полутора миллионов человек. Больше всего эвакуаций было проведено 19 декабря 2019 г. – тогда были эвакуированы около 170 тысяч человек. 27 января 2019 г. анонимные угрозы поступили более чем в 700 учреждений, за день были эвакуированы более 16 тысяч человек[1]. Каков материальный ущерб всех этих эвакуаций – остается только догадываться.

Кондраткова Н.В.,

кандидат экономических наук, доцент
Новосибирский филиал Московской академии СК России

Коптев А.Ю.

Управление Федеральной налоговой службы России по Новосибирской области

Взаимодействие как основа противодействия экономической преступности

В рамках противодействия уголовному преследованию лица, уклоняющиеся от уплаты налогов, осуществляющие рейдерские захваты, легализацию, совершающие обналичивание и иные экономические преступления, маскируют свою противоправную деятельность под гражданско-правовые отношения. Посредством фирм-однодневок обнальщики и недобросовестные налогоплательщики создают фиктивный документооборот и видимость реального совершения финансово-хозяйственных операций, рейдеры скупают задолженность компаний и завладевают их активами через процедуру банкротства, наркоторговцы легализуют преступные доходы посредством «QIWI-кошельков» и так далее. Механизм совершения указанных преступлений, помимо создания фирм-однодневок, предполагает совершение и иных противоправных деяний (например, незаконное использование документов для образования юридического лица, фальсификация ЕГРЮЛ, фальсификация решения общего собрания и прочие), что определяет необходимость комплексного подхода к противодействию экономической преступности и потребность взаимодействия правоохранительных и контролирующих органов.

В частности, невозможность автономного аккумулирования, сбора, анализа и оценки информации обуславливает взаимодействие следователя с Федеральной налоговой службой России, осуществляемое на

[1] Анонимы продолжили волну лжеминирований с нового почтового адреса // Интерфакс : международная информационная группа : официальный сайт. URL: https://www.interfax.ru/russia/692953 (дата обращения: 29.01.2020).