ВОЙНА В УСЛОВИЯХ МИРА

В.В. УСТИНОВИЧ,
начальник Управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь, полковник милиции

По оценкам Министерства внутренних дел Республики Беларусь, в 2017 г. по сравнению с предыдущим годом количество выявленных преступлений в сфере высоких технологий увеличилась более чем на 25 % – с 2471 до 3099. Рост этого вида криминала произошел за счет киберпреступлений против информационной безопасности.

Приведенные выше показатели, а также общее состояние в сфере информационной безопасности в белорусском сегменте сети интернет мы попросили прокомментировать начальника Управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь, полковника милиции Вадима Викторовича УСТИНОВИЧА.

В компетенцию МВД Республики Беларусь входят вопросы правоохранительной деятельности в сфере информационной безопасности. Но пользователям интернета хорошо известно, что киберпреступления могут принимать множество форм. Например, на электронные почтовые ящики нередко приходят сотни писем с абсурдными предложениями: скажем, отправить платное SMS-сообщение, чтобы избавить компьютер от вирусов или зайти на сайт социальной сети, и т. д. По расчетам экспертов ООН, от киберпреступлений ежегодно страдает более 1,5 млрд человек в 233 странах.

Следует заметить, что в мире наблюдается определенная взаимосвязь: по мере развития технологического оснащения и формирования сети растут масштабы совершаемых преступлений. На счету правоохранительных органов есть немало примеров установления отдельных киберпреступников и преступных групп, но очевидно, что проблема не решается просто путем задержаний. Назрела прямая необходимость повышения уровня взаимодействия, как международных организаций, так и отдельных ведомств внутри стран. Ведь на сегодняшний день информационные технологии способны определять степень национальной безопасности и суверенитет отдельных государств.

Уже давно IT-технологии стали неотъемлемой частью практически всех операций с деньгами – это и миллионные расчеты,

и оплата обычных услуг вроде коммунальных. Всем понятно, что платить в один клик весьма удобно, но люди и бизнес должны быть уверены, что транзакция состоится, деньги не украдут. Поэтому защита средств является ключевым вопросом современного кредитно-финансового оборота, особенно при переходе от наличных расчетов к электронным платежам. Известно, что кибермошенники атакуют не только электронные кошельки конкретных владельцев, но и вообще все элементы кредитно-финансовой системы, счета банков, финансовых компаний. Они стремятся в первую очередь изучить уязвимость программного продукта, тем более что любой из них создается людьми, а значит, возможны «бреши». Существует и просто использование обычной человеческой доверчивости. Например, имея в своем распоряжении персональные данные, хакеры получают возможность для различного рода противоправных действий. По украденным паспортным данным нередко оформляют поддельные договоры, а сведения, составляющие врачебную тайну, могут дискредитировать человека или стать причиной вымогательства.

Вот одна из историй задержания киберпреступника в нашей стране. В ходе оперативно-разыскных мероприятий был установлен житель Гомельской области, причастный к распространению через интернет-форум damagelab.org вредоносной программы «Андромеда». По сведениям компании «Майкрософт», «Андромеда» являлась одной из самых реализуемых и распространенных программ, которой было заражено более 3,5 млн компьютеров. Данная программа использовалась для создания и управления ботсетью, неправомерного завладения компьютерной информацией, установки на компьютере жертвы иных вредоносных программ. В ноябре минувшего года в результате проведенной операции подозреваемый задержан. Возбуждено уголовное дело по части 2 статьи 354 УК Республики Беларусь.

Более двух третей преступлений, выявленных в ИТ-сфере, относятся к хищениям путем использования компьютерной техники. В таких случаях уголовная ответственность предусмотрена в статье 212 УК Республики Беларусь.

Компетентные органы отреагировали и на другие противоправные действия в сети интернет. Реальный масштаб борьбы с киберпреступлениями в Беларуси отражают конкретные показатели. Например, в 2017 г. по сравнению с предыдущим годом число выявленных преступлений в сфере высоких технологий увеличилось на 25,3 % – с 2471 до 3099. Общий уровень раскрываемости несколько снизился и составил 53,6 % (2016 г. – 56,5 %). Тем не менее тревожный звонок настиг многих киберпреступников. К уголовной ответственности привлечено 956 человек. Среди них 294 имеют судимость, 683 не работают и не обучаются, 34 являются несовершеннолетними. Установленный материальный ущерб составил 3,2 млн рублей, из которых возмещена почти половина.

Самый беглый анализ показывает, что увеличение количества киберпреступлений произошло за счет прироста криминальных действий против информационной безопасности (на 20 %, с 651 до 781). Их удельный вес от общего числа вскрытых преступлений в сфере высоких технологий составил 25,2 %. При этом значительно возросло количество фактов несанкционированного доступа к компьютерной информации. Более двух третей преступлений, выявленных в ИТ-сфере, относятся к хищениям путем использования компьютерной техники. В таких случаях уголовная ответственность предусмотрена в статье 212 УК Республики Беларусь.

Особенный рост количества киберпреступлений происходит на просторах социальных сетей. Нередко главной мотивацией для преступников служит беспечность самих пользователей сети, их пренебрежение элементарными правилами защиты. Регламентам безопасности в интернете посвящено множество статей. Для ясности: речь не о глобальной киберозабоченности, а самых элементарных, но неизменно актуальных для каждого пользователя правилах. Приведем некоторые из них.

✓ Не отвечайте на сообщения с просьбами о помощи больным людям или животным и уж тем более не перечисляйте им денежные средства! Если вы действительно хотите помочь, то обратитесь в фонды помощи, которые зарегистрированы в Республике Беларусь, информация о них размещена на их официальных сайтах.

✓ Ни в коем случае не реагируйте на странные сообщения от друзей, в которых они просят перевести им денежные средства. Если уж вы переживаете за своего друга либо близкого человека, то позвоните ему и спросите, что именно случилось.

✓ Не отвечайте на сообщения о том, что с вашего счета пытаются списать денежные средства, не переходите по ссылкам, которые отправляют мошенники. Если у вас действительно появились сомнения, то позвоните на горячую линию банка, только ни в коем случае не звоните по номеру телефона, указанному в ссылке либо в сообщении!

✓ Если вы не хотите, чтобы ваша личная жизнь и откровенные фото стали достоянием общественности, не делитесь этим с незнакомыми людьми.

✓ Придумывайте оригинальный и сложный пароль для почтового ящика, на который вы будете регистрировать аккаунт социальной сети. Всегда устанавливайте разные пароли при регистрации на различных интернет ресурсах. Если вам сложно запомнить пароли, сохраняйте их в недоступном для посторонних лиц месте.

✓ Если желаете приобрести что-либо через интернет, не вносите предоплату. Уважающий себя продавец берет оплату за товар после того, как клиент получит его на почте либо в офисе продаж такого магазина.

Нельзя обойти вниманием вопросы информационной безопасности в связи с активным продвижением электронных порталов госуслуг, которые содержат информацию о гражданах, а также созданием различных электронных баз данных, реестров и кадастров. К примеру, в процессе развития «интернета вещей» на первый план выходят вопросы безопасности оказания услуг «умный дом» и сопутствующих IT-проектов. Бесспорно, их защищенность должна обеспечиваться организацией, оказывающей данный вид сервиса. В свою очередь потенциал безопасности «умного» оборудования должен предусматриваться еще на стадии его разработки и производства, т. е. производителем. Потребитель «умного» оборудования также обязан понимать меру ответственности за соблюдение условий эксплуатации такого оборудования в соответствии с правилами, установленными производителем.

Суть проблемы киберпреступлений – зло огромного масштаба, которым движет элементарная корысть. С большой долей вероятности к ним могут добавиться новые угрозы, направленные на завладение криптовалютой, новые виды интернет-мошенничества и вредоносные программы.

По мнению экспертов, таким угрозам должно противостоять тотальное внедрение эффективных систем защиты сетей и данных. Дело это непростое, однако к вопросам информационной безопасности важно подходить продуманно, ответственно и с учетом человеческого фактора.