ТЕХНОЛОГИИ

Компьютер и оперская смекалка

С таким «арсеналом» полицейские борются с киберпреступностью

Скромная красноярская домохозяйка за два года заработала около трех миллионов рублей, взламывая интернет-ресурсы. Работала «хакерша» только с проверенными клиентами. Но однажды в их число незаметно затесались полицейские. Женщине предложили достать реквизиты «ящика», который специально для этого был создан, а когда та выполнила заказ, перечислили на ее счет в виртуальной платежной системе оплату – две тысячи рублей. После проведенного комплекса оперативно-разыскных мероприятий стражи порядка нагрянули к изобретательной даме с обыском, который и помог установить примерные объемы ее криминально-интеллектуального бизнеса. Пока доказано 39 эпизодов (на те самые три миллиона), но оперативники уверяют, что в реальности их было более сотни… Против «взломщицы» возбуждено уголовное дело по статье, карающей за использование вредоносных компьютерных программ.

Выследили мошенницу сотрудники так называемого отдела «К» ГУ МВД России по Красноярскому краю, который специализируется, если говорить кратко, на выявлении и раскрытии преступлений в сфере информационных технологий. И, разумеется, это дело – одно из многих. В чем особенности борьбы с киберпреступностью? Об этом рассказывает начальник подразделения подполковник полиции Вячеслав ЛАПИН.

– Информационные технологии прогрессируют стремительно. То, что совсем недавно считалось «последним писком», сегодня – вчерашний день. Здесь уместно вспомнить – с чего все начиналось?

– Начало активной работы по борьбе с преступлениями в сфере информационных технологий можно отнести к концу 90-х годов прошлого века. Характерным признаком того времени было широкое распространение различных несертифицированных радиоэлектронных и специальных технических средств, использование которых создавало помехи и приводило к нарушению работы гражданских и военных радиоэлектронных систем. Для борьбы с их незаконным оборотом в 1998 году в структуре МВД был создан отдел «Р». Затем в связи с увеличением направлений деятельности и количества задач отдел «Р» был преобразован в управление по борьбе с преступлениями в сфере высоких технологий. В 2001 году в ходе реорганизации в правоохранительных органах управление было преобразовано в отдел «К» ГУВД по Красноярскому краю. В этот период сформировались следующие направления деятельности отдела: по предупреждению, пресечению и раскрытию компьютерных преступлений, борьбе с незаконным оборотом радиоэлектронных и специальных технических средств, предназначенных для негласного получения информации, и с незаконным доступом к услугам и ресурсам связи. Также в числе задач – противодействие посягательствам на интеллектуальную собственность, на неприкосновенность частной жизни, борьба с распространением в Интернете материалов порнографического содержания, в том числе с участием несовершеннолетних.

– Что изменилось, когда прошла «мода» на запрещенные радиоэлектронные средства?

– В 2000 году начался следующий период, занявший примерно семь лет. Тогда основным компьютерным преступлением стала кража логина и пароля, то есть воровство собственно Интернета, который тогда стоил дорого. В то время, как вы помните, было модемное соединение, связанное с телефонными линиями, и учет велся не по объему скачанной информации, а по времени, проведенному в Сети. «Технология» таких махинаций, по сути, была одна – чужие логины и пароли получали при помощи вредоносной программы с незащищенного компьютера, копировался файл, содержащий зашифрованные реквизиты, которые потом расшифровывали. Потерпевшие, обнаружив, что их временной лимит вдруг исчез, обращались к провайдерам, а те – к нам. Установить в то время злоумышленника было не так уж и сложно.

– А потом через Интернет пошло все…

– Совершенно верно. Теперь через Сеть можно совершать что угодно – от обычных покупок до банковских операций. Но отношение пользователей к защите своих компьютеров принципиально не изменилось. Многие все еще думают, что неприятности могут случиться с кем угодно, только не с ними, экономят на защите, забывая, что потери несопоставимы с ее стоимостью. Таким образом, примерно с 2007 года наступил новый этап, который продолжается и по сей день. Основа та же – воровство логина и пароля, но теперь это дает возможность практически для любых действий, начиная от доступа к банковским счетам до взлома личных страничек в соцсетях, чтобы компрометировать ее владельца, рассылать от его имени угрозы, оскорбления и прочую негативную информацию. Вообще кража реквизитов дает доступ к практически любым действиям с чужим компьютером. Поэтому в последнее время сама киберпреступность стала более организованной, а размеры ущерба возросли кратно – в случае хорошо подготовленных киберпреступлений это миллионы рублей.

Киберпреступность стала более организованной, а размеры ущерба возросли кратно – в случае хорошо подготовленных киберпреступлений это миллионы рублей

– Можно ли обозначить общий объем преступлений в денежном выражении?

– Такой статистики нет. Отдел выявляет порядка 170 преступлений в год, но это не всегда махинации с деньгами, а в целом преступления в сфере информационных технологий.

– Какие наказания грозят киберпреступникам?

– Если говорить о «классике жанра» – хищении логина и пароля, то это 272-я статья УК РФ. Она небольшой тяжести и предусматривает в основном незначительное наказание – обычно суд назначает условный срок лишения свободы или ограничивается штрафом. Кроме того, многие квалифицирующие признаки, например совершение преступления группой лиц по предварительному сговору и прочее, здесь не работают, поскольку в этой области, как правило, действуют одиночки, не афиширующие свою деятельность. Хотя законодательство меняется. Так, с недавнего времени введена статья 159.6 – мошенничество в сфере компьютерной информации, – предусматривающая более тяжкое наказание. В практике отдела есть раскрытое преступление, связанное со взломом компьютерной сети, когда злоумышленник весь период следствия – восемь месяцев – находился под стражей.

– Кто кого догоняет – вы преступников или они вас?

– Однозначно сказать нельзя. Все наше «вооружение» – компьютер, Интернет, бумага, ручка и оперская смекалка. Особенность подразделения в том, что у нас работают сотрудники, имеющие специализированное образование в сфере IT-технологий и информационной безопасности. Такое сочетание опера и технаря дает положительные результаты. Что касается материально-технического обеспечения, то здесь проблем нет. Но стоит остановиться на проблемных вопросах. Прежде всего они связаны с трансграничностью функционирования Интернета, что затрудняет процесс обмена необходимой информацией, обеспечивающей оперативное реагирование на факты преступных посягательств. Наиболее часто используемые для совершения преступлений сервисы и службы территориально могут находиться в различных субъектах России или за рубежом. Работа с ними осуществляются удаленно, не требует подтверждения персональных данных пользователя и, как правило, занимает у злоумышленников небольшой промежуток времени. Процесс же документирования и раскрытия информационного преступления основан на механизме официального документооборота между правоохранительными органами и поставщиками интернет-услуг и значительно растянут по времени.

– Сейчас полиция делает ставку на людей с высшим образованием. Но у вас, наверное, требования еще жестче?

– Требования к сотруднику отдела «К» в части физической, специальной и морально-психологической подготовки ничем не отличаются от требований к офицеру полиции других подразделений. Костяк отдела сформировался давно. В основном это выпускники Сибирского юридического института, отработавшие определенное время в оперативных подразделениях, имеющие опыт агентурно-оперативной работы. Я сам начинал службу в ОВД с оперативника уголовного розыска. Это собственно база, а специальные знания получали в процессе работы. На начальном этапе каких-либо методических рекомендаций не было. Приходилось разъяснять работникам следственных подразделений, судебных органов премудрости нового вида преступлений. Но сейчас уже наработана серьезная следственная и судебная практика, разработаны и распространены методические рекомендации Управления «К» МВД России по выявлению и документированию информационных преступлений на основе передового опыта. В последнее время преступлениям в сфере высоких технологий уделяется все больше внимания, видимо поэтому в ходе реформы МВД подразделение «К» в Красноярске не подверглось сокращению.

Иван ПЕТРОВ