Илья Сачков: «Самая большая проблема компьютерной преступности в том, что общество не совсем верит в реальность высокотехнологичных правонарушений»

*Илья **Сачков** — генеральный директор и основатель компании «Group-IB», член Экспертного совета ПИР-Центра — выступил на круглом столе **«Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса»,** проведенном на площадке Комитета гражданских инициатив, и рассказал о масштабах финансовых киберпреступлений: по данным компании, годовой оборот высокотехнологичной преступности в России и СНГ оценивается более чем в 3 трлн рублей.*

«Пульс Кибермира» публикует полный текст выступления эксперта. Другие материалы круглого стола выйдут в следующем номере журнала «Индекс Безопасности».

Постараюсь очень кратко рассказать о трендах развития высокотехнологичной преступности, которые мы видим на территории Российской Федерации, потому что часть нашей работы в *Group IB* — это экспертно-криминалистическая деятельность по сопровождению особо сложных и резонансных уголовных дел против компьютерной преступности. Важно понимать, кто стоит по ту сторону закона, как они работают, и сделать так, чтобы закон их мог наказать.

Самая большая проблема компьютерной преступности состоит в том, что общество в целом не совсем понимает, о чем идет речь, и не совсем верит в

реальность высокотехнологичных правонарушений. Потрясающий пример: у нас есть список зараженных вредоносным ПО бухгалтерских компьютеров различных российских юридических лиц с указанием похищенных у них денежных средств. В их числе управление делами президента Российской Федерации, *Тройка Венчур Кэпитал* и многие другие серьезные организации.

Интересный пример произошел с Московской биржей. В апреле мошенники от лица *Энергобанка* отправили на биржу заявку в размере 300 млн долл. и получили деньги. Банк обратился к нам за помощью, мы провели компьютерную криминалистическую экспертизу и нашли на компьютере, на котором находился терминал, вредоносное программное обеспечение, созданное для атак на брокерские терминалы. После этого мы получили запрос из Центрального банка России с требованием предоставить все материалы по делу, которые на самом деле являются тайной следствия, что мы и ответили Центральному банку. В ответ получили штраф в 500 тыс. рублей за нарушение закона об инсайдерской деятельности. В итоге Центральный банк не верит в то, что заявку мог отправить вирус, в отношении *Энергобанка* ведется проверка, а у нас серьезные проблемы: мы заплатили штраф 500 тыс. рублей. Уголовное дело продолжается.

Говоря о компьютерной преступности, важно понимать, что общество знает лишь о верхушке айсберга. Возьмем пример *кардинга* — воровства денег с кредитных карточек — это несложное и очень популярное преступление. Преступники пользуются специализированными магазинами, в которых продаются *дампы* кредитных карточек — копии магнитной полосы и PIN-код, то есть то, что необходимо, чтобы снимать деньги с карточки. Набор дампов стоит порядка 10 долл. В одном магазине продается около 5 млн валидных кредитных карточек. Принято думать, что теневой интернет — это что-то очень технически сложное, но на самом деле — ничего подобного. У

таких магазинов очень удобный интерфейс, они мало чем отличаются от обычных интернет-магазинов кроме товара. Когда правоохранительные органы видят подобные сайты в интернете, они пытаются их блокировать. Проблема в том, что, закрывая что-то в интернете без понимания существующих тенденций и того, как с ними бороться, правоохранители просто запускают *гонку вооружений*. Ведь люди, которые создают кардинговые магазины, из-за того, что закрыли их веб-сайт, ликвидировали домен, который стоит 20 долл., не расстроятся и не скажут: «Пора, наверное, отходить от дел». Напротив, они станут умнее, хитрее, будут использовать новые средства анонимного доступа. Так, кстати, произошло с торговлей наркотикам. Изначально сайты, на которых их продавали, находились в обычных доменных зонах, а продавцов было достаточно легко идентифицировать. После принятия закона о блокировке эти сайты начали тысячами закрывать, а наркоторговцы ушли в теневой интернет. Проблема никуда не делась, но преступники стали изобретательнее, и теперь есть случаи (ФСКН, естественно, в курсе), когда наркотики заказывают с доставкой на дом через *Почту России*.

Сталкиваясь с преступлениями в интернете, очень важно анализировать всю цепочку. В случае с кардингом надо начинать с вопроса откуда преступники берут информацию. Каким образом похитили данные 5 миллионов карточек? В магазине, о котором я говорил, продавали дампы, полученные с зараженных терминалов в двух американских торговых сетях, *Target* и *Home Depot.* В первой похитили данные 70 млн карточек, во второй — 56 млн. Это очень важная информация, ведь если мы знаем точку компрометации, понятно, что делать дальше: любой человек, который был в этих торговых сетях в определенный промежуток времени, должен свою карточку заблокировать.

Также важно понимать, что, владелец сайта, торгующего дампами, на комиссии с каждой покупки заработал 6 млн долл., и в случае юридического преследования на эти деньги он обеспечит себе первоклассную юридическую защиту, самых лучших адвокатов. Уже появляется целый класс адвокатов, которые специализируются на защите компьютерных преступников, потому что это достаточно просто и очень прибыльно.

Для нас главное — это понять, кто занимается подобными преступлениями. Возьмем самого крупного продавца в этом магазине, который продал 150 тыс. карточек и заработал 1 млн долл. На хакерских форумах его зовут Rescator, а в жизни — Андрей Ходыревский. Сейчас он находится в международном розыске. Злоумышленники очень любят глумиться над обществом: его база данных с карточками называется *Антиамериканские санкции*, то есть это ответ киберпреступности на американские санкции, так как все пострадавшие от его действия банки — это, известные, крупные американские банки.

Что происходит сейчас на рынке компьютерной преступности? Каковы цели злоумышленников? В первую очередь это деньги. Есть случаи, когда компьютерные преступники охотятся за информацией, но это сотые доли процента. Благодаря развитию платежных систем, интернет-банкинга для физических и юридических лиц процветает воровство денег в платежных системах. Технически это относительно несложно, а если добавить к этому сверхприбыль и чувство безнаказанности, получается привлекательная для правонарушителя картина.

Надо иметь в виду, что компьютерный преступник не вызывает в обществе негативных эмоций в отличие, например, от человека, который продает наркотики. Кроме того, юристы не успевают за развитием высокотехнологичных преступлений, и в законодательстве много лакун.

Компьютерные преступления можно за одну секунду совершить с территории одной страны через территорию другой страны в ста странах одновременно. Поэтому, несмотря на то, что государство, общество, бизнес, люди тратят на информационную безопасность с каждым годом все больше, атак меньше не становится.

Отношение общества — это отдельный вопрос. Приведу старый, но показательный пример. Господин Аникина из Новосибирска в составе организованной преступной группы украл 9,5 млн долл. В том же году российские суды рассматривали еще два уголовных дела: господин Блинников взломал щит на Садовом кольце в Москве и *крутил* там порнографию, а господин Гаврилов украл у своей соседки с дачного участка два куста роз и два куста лилий. Приговоры, вынесенные в отношении этих людей: Аникин — пять лет условно, Блинников — шесть лет колонии, Гаврилов — два года строгого режима. В сознании людей кража электронных денег — это своего рода игра, поэтому для преступников гораздо выгоднее заниматься тем, что непонятно и у чего нет негативной окраски. Кстати, *Первый канал* в день оглашения приговора Аникину выпустил новость под заголовком «Талантам молодого программиста удивился американский банк». Мы мониторим хакерские форумы, и в этот день количество регистраций на них увеличилось на 400% — то есть, во столько раз увеличилось количество людей, которые благодаря телевизионщикам заинтересовались тематикой компьютерной преступности.

Появляется целое поколение людей, которые, в отличие от поколения 90-х, даже не учатся информационным технологиям, а просто используют готовые, понятные инструменты. Они как правило очень молодые — до 30 лет. Во многих случаях их родители даже не подозревали, чем занимаются дети. Программы, которыми они пользуются, предельно просты и, что самое

поразительное, все они имеют лицензионную политику, и создающие их злоумышленники тратят время на борьбу с пиратством и на защиту своей собственности. Каждый разработчик имеет круглосуточную техподдержку на нескольких языках, которой могут позавидовать некоторые производители программного обеспечения. Использование такого *софта* не требует никаких технических знаний. Есть, конечно, в составе преступных групп очень умные люди, но есть и те, у которых IQ в районе 40-60.

Члены преступной группы зачастую живут в разных регионах не только России, но и мира, что создает кучу юридических проблем. Если группа находится в трех-четырех странах, то, к сожалению, о расследовании и кооперации правоохранительных органов можно забыть. Сейчас многие люди, которые подпадают под подозрение в совершении компьютерных преступлений в России, уезжают на Украину, а многие хакеры с Украины приезжают в Россию. Россияне с территории Украины воруют деньги в российских банках, украинцы с территории России воруют деньги в украинских банках, и никто никого не трогает. Политика используется для того, чтобы скрывать компьютерные преступления. Есть и другие факторы. Кроме технической возможности заразить компьютеры, преступники ищут страны, где нет проблем с обналичиванием денег. В России это относительно просто, поэтому компьютерная преступность процветает. Решение вопроса с *обналичкой* нанесло бы очень эффективный удар по компьютерной преступности.

Еще одна проблема — мобильные устройства. Благодаря тому, что *Android* занял 80% мирового рынка устройств, и телефоны на базе ОС *Android* продаются за 20 долл., идет огромное количество разработок вредоносного ПО под мобильные устройства. С телефоном можно сделать все, что угодно: начиная от кражи денежных средств и заканчивая прослушкой телефона,

когда он просто лежит на столе. Стоимость заражения телефонов на черном рынке — приблизительно 100-200 долл. за одну тысячу аппаратов.

Мы регулярно, с 2006 г. выпускаем памятки по компьютерной гигиене, но есть ощущение, что их читают только наши сотрудники. В прошлом году мы приходили с инициативой в Министерство образования и предлагали часть школьного курса «Основы безопасности жизнедеятельности» выделить под правила компьютерной гигиены. К сожалению, это не получилось. В то же время в США дети 6-8 лет изучают основы компьютерной грамотности. При этом им говорят: «Ваш телефон, ваш компьютер — элемент национальной безопасности». В 6-8 лет они знают, что такое *фишинг, кардинг*. Я считаю, то же самое необходимо в России, потому что человек, будучи школьником, потом становится сотрудником предприятия, и не зная вот этих вещей, он, конечно же, будет подвергаться атакам.