ЕСТЬ РЕШЕНИЕ

Формы противодействия кибератакам и социальной инженерии в кредитно-финансовой сфере

С 13 ПО 17 МАЯ в Московском университете МВД России имени В.Я. Кикотя состоялась КОНФЕРЕНЦИЯ ДЛЯ СОТРУДНИКОВ ГСУ ГУ МВД РОССИИ ПО Г. МОСКВЕ.

Программа мероприятий была очень насыщенной и интересной. В рамках форума обсуждался широкий спектр наиболее актуальных вопросов, среди которых:

- современный опыт в организации расследования дистанционных преступлений;
- анализ актуальных схем мошенничества в системе дистанционного банковского обслуживания;
- передовой опыт использования систем распознавания лиц в России;
- противодействие социальной инженерии в кредитно-финансовой сфере;
- криминалистические аспекты расследования дистанционных хищений денежных средств и другие.

Участники конференции получили сертификаты о повышении квалификации по направлению «Расследование хищений денежных средств, совершенных дистанционным способом».

В рамках живого диалога и обмена практическим опытом участники конференции выступили перед аудиторией со своей, порой неожиданной, точкой зрения на криминальные вызовы, существующие не только в кредитно-финансовой сфере, но и в области

DEPOSITPHOTOS.COM/KARPENKOLIA

МИХАИЛ НИКИТИН,
преподаватель учебного центра «Информзащита»

информационно-телекоммуникационных услуг, в сфере обработки персональных данных, информационной безопасности и других электронных сервисов. Одна из наиболее интересных дискуссий разгорелась вокруг выступления спикера от Учебного центра «Информзащита», автора данной статьи. Он предложил участникам конференции, многие из которых имеют право вносить на рассмотрение уполномоченных структур законодательные инициативы, ужесточить российское законодательство в части противодействия преступлениям информационно-коммуникационной направленности. По его мнению, существующих мер оперативного реагирования в самом уязвимом сегменте российской экономики – в кредитно-финансовой сфере, явно недостаточно, т. к. действующее законодательство явно пробуксовывает, не успевая за новыми модификациями мошеннических схем. Бесконечные модернизации отдельных статей особенной части УК РФ (158, 159) не удовлетворяют правоохранительные органы своей достаточно узкой квалификацией в описании составов преступлений, связанных с хищениями денежных средств дистанционным способом. Из-за этого правоприменительные органы, которые в пределах своей компетенции правомочны налагать административную, уголовную ответственность на юридических и физических лиц, не имеют достаточно устойчивой правовой позиции для вынесения законных решений, т. к. квалифицирующие признаки таких уголовных деяний не конкретны или размыты, а порой и вовсе не соответствуют по описанию конкретной норме статьи.

Вызывают недоумение и легкую растерянность меры уголовной ответственности за преступления данной направленности, где установленные сроки уголовного наказания просто «умиляют»! Например, ограничение свободы до двух лет, принудительные работы и лишение свободы на тот же срок по ч. 1, ст. 159 УК РФ! Давайте просто сравним: в США для хакеров, которые причиняют ущерб защищенным абонентским компьютерам и совершают различные мошеннические действия, в которых компьютер выступает лишь как орудие преступления, предусмотрены сроки наказания, которые колеблются от 10 до 25 лет лишения свободы. Нельзя не отметить и такой факт, что в США компьютерные преступления причиняют ущерб, на порядок превышающий ущерб от других категорий преступлений. Интересна в этом плане статистика, опубликованная экспертами.

С апреля 2017 года по декабрь 2018 года продолжались атаки на интернет-портал Click2Gov, принимающий платежи за парковку, коммунальные и другие муниципальные услуги в США. За этот период было зафиксировано 20 подобных инцидентов, приведших к утечке конфиденциальной информации не менее чем с 111 860 платежных карт. Предполагается, что злоумышленники загружали на веб-серверы JSP-оболочку SJavaWebManage и в режиме отладки получали доступ к данным банковских карт в незашифрованном виде.

https://www.ptsecurity.com/ru-ru/research/analytics/cybersecuritythreatscape-2018-q4/

Самый обсуждаемый вопрос касался компетенций современного следователя. А именно, его профессиональных качеств, личной грамотности, способности быстро и безошибочно разбираться в тех вопросах, которые находятся далеко за пределами его юрисдикции, но непосредственно связанные с ними. Сегодня стало понятно, что одних знаний юриспруденции современному следователю явно недостаточно, так как в «тело» основного состава преступления часто бывают вплетены дополнительные отягчающие обстоятельства, например, из области криминальной биоинженерии, торговли человеческими органами, людьми, незаконного оборота наркотических и психотропных веществ, включающих в себя следы наркотрафика, незаконного оборота оружия и т. д., которые усложняют и одновременно увеличивают сроки расследования.

В этой связи нами было высказано предложение о создании в ФЗ № 63 от 13.06.1996 г. отдельной, XIII главы, где был бы собран весь наработанный оперативно-следственный опыт. Это позволило бы судам сконцентрировать внимание на данной проблеме путем обзора судебной практики в соответствующих профильных журналах, бюллетенях, публикациях. Впоследствии это помогло бы им квалифицированно и безошибочно разбираться в непростых вопросах, связанных подобной категорией преступлений.

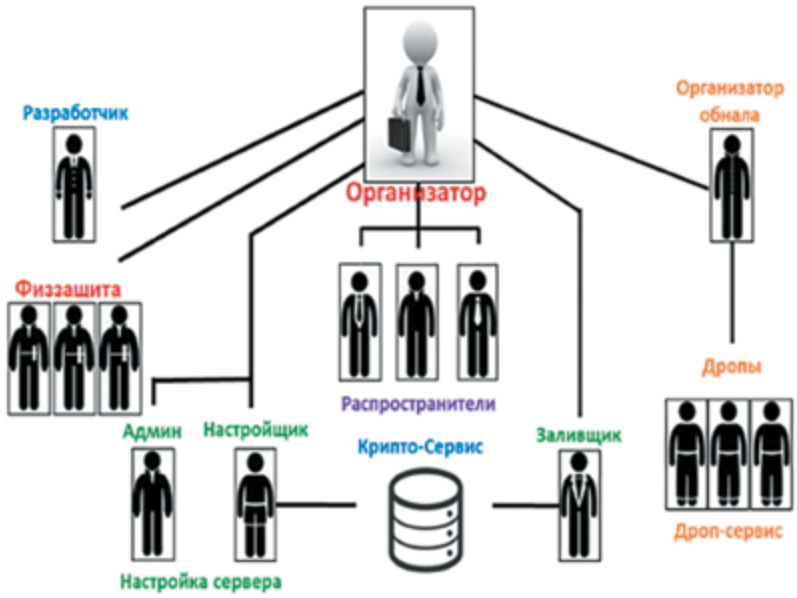
Оживленный диалог вызвала тема ответственности коммерческих и государственных компаний за некачественный контент электронных услуг, сервисов и приложений, которые не прошли у разработчика глубокой проверки на уязвимость. Получается, что созданный и включенный в контент провайдера программный продукт с самого начала разработчиком не исследовался на негативные побочные свойства. Вместо него с большим успехом это стали делать злоумышленники, выискивая уязвимости в электронных сервисах разработчика, создавая на их основе мошеннические схемы, нацеленные на карман потребителя некачественного контента. Из-за этого у населения стало развиваться недоверие к электронным кредитно-финансовым инструментам государственных и коммерческих финансовых организаций. В итоге, возросла нагрузка на правоохранительные органы, которые обязаны реагировать на обращения граждан и расследовать запутанные мошеннические схемы из-за того, что сам разработчик не удосужился довести свой продукт до совершенства. За рубежом подобных инцидентов нет, либо встречаются крайне редко, так как разработчик сервиса несет полную ответственность за свой продукт перед законом, а меры уголовной ответственности, например, в США, не сравнимы с российскими по степени тяжести.

Анализ сегодняшней криминогенной обстановки в кредитно-финансовом секторе экономики, в области информационно-телекоммуникационных услуг, информационной безопасности и различных электронных сервисов дает понимание о том, что социальная инженерия и кибермошенничество, ранее существовавшие более или менее разобщенно, трансформировались и объединились в более сложный тандем. Сложился некий организованный преступный союз, со своей жесткой внутренней иерархией, закрытой областью сетевых коммуникаций (darknet), соединения в котором устанавливаются только между доверенными пирами с использованием нестандартных протоколов и портов. Такая форма существования ими выбрана неспроста. Преступники уже почувствовали, что правоохранители наступают им на пятки и хвосты, поэтому инстинкт самосохранения подсказал им объединиться в целях выживания. Яркие примеры успешных оперативных мероприятий есть, и положительных результатов все больше. Более того, ощутив на себе нисколько не ласковые формы и методы ОРД силовиков, жулики стали как-то приспосабливаться к этой неуютной среде обитания. Многие из них перебрались в ближнее зарубежье под крыло своих заказчиков из теневого бизнеса. Не секрет, что в некоторых странах бывшего СССР местные федералы с киберпреступностью сталкиваются нечасто. А оставшиеся на своей родине хакеры освоили методы конспирации и бдительной осторожности, понимая, что один прокол с их стороны и последствия оперативного вторжения будут для них непредсказуемы.

Поэтому преступники стали действовать ювелирно, без права на ошибку. Главное и основное свойство современных преступных сообществ заключается в удаленности друг от друга и в отсутствии каких бы то ни было физических контактов. В основе их коммуникаций – персональная изолированность, так называемый принцип NONAME. С одной стороны, это обеспечивает им гарантию неопознанности членами внутри своей преступной группы и иными соучастниками в ходе предварительных следственных действий. Однако, с другой стороны, в случае «поиска правды» в своей криминальной среде эта анонимность их заводит в тупик. Известно, что разработчиков вредоносного ПО или чего-то криминально-подобного «кидают» свои же, либо «авторитетные» заказчики. Более того, многих из них используют «втемную» не раскрывая истинных целей кибератаки, а потом, в случае «заметания» следов, просто сводят счеты с каждым по отдельности в силу разобщенности преступной группы (см. схему.).

И еще, надо понимать, что сегодня такие преступные сообщества разбросаны по всему миру. Их местонахождение регулярно меняется, их проекты финансируются воротилами теневого бизнеса, а их действия нацелены не только на обрушение инфраструктуры какой-либо

СХЕМА ПРЕСТУПНОЙ ГРУППЫ



Они могут и знают все или почти все по части слежки, физзащиты людей,объектов, прекрасно владеют практически всеми видами оружия, навыками рукопашного боя, и т. д.

корпорации-цели. Часто их действия направлены на создание благоприятных условий для смены власти и установления своего режима правления в небольших странах, путем организации так называемых «цветных революций». Несложно догадаться, что в их рядах есть специалисты не только из киберсреды. В состав таких бригад входят опытные универсальные стратеги из числа бывших силовиков различных федеральных структур. Они могут и знают все или почти все по части слежки, физзащиты людей, объектов, прекрасно владеют практически всеми видами оружия, навыками рукопашного боя, и т. д. Это не те молодые и худосочные «ботаники» – разработчики, а достаточно свирепые боевики, с которыми простому неподготовленному человеку лучше не встречаться. За их плечами богатый профессиональный опыт, насыщенный примерами выхода из сложнейших нестандартных ситуаций. В случае опасности они обладают молниеносной защитной реакцией, которая срабатывает на подсознательном уровне, но самое главное – они обучают этим знаниям, навыкам и приемам своих сообщников. В результате подобной трансформации кибернаутов и силовой поддержки появились еще более изощренные способы дистанционного мошенничества. Эти преступные организации используют современные атакующие компьютерные технологи в совокупности с методами социальной инженерии, граничащие с угрозой физического насилия, поэтому защититься от подобных преступлений становится крайне затруднительно. Пожалуй, сегодня никто в мире не имеет полной статистической и прогнозируемой картины преступности такого формата. Государственные и коммерческие структуры, которые когда-либо подвергались подобным преступным посягательствам, не очень склонны афишировать сведения о причиненном материальном или физическом ущербе, поэтому случаи совершения подобных преступлений становятся публично известными далеко не всегда. Но даже те факты, которые становятся достоянием гласности, производят сильное впечатление.

Такая беспомощность правоохранителей и беззащитность населения России связана, как ни странно, с нашим действующим российским законодательством, а точнее, с его «беззубостью». Если сравнить диспозиции некоторых статей УК РФ – ст. 159, 272, 273, 274 (действующая редакция 2018 г.) и Раздел 18 Примерного УК США 1986 г., параграфы 1029, 1030 и 1362, то становится понятно, почему российским кибер-синжерам так… «легко и весело живется на Руси». Уместно выделить из ряда мер по усилению борьбы с киберпреступностью в США норму ст. 814 «Акта Патриота» (USA PATRIOT Act 2001, упраздненный в 2015 году, вместо которого введен «Акт о свободе»), которая вносит множество изменений в параграф 1030 Раздела 18 Свода законов США от 1986 г. («Акт о компьютерных мошенничествах и иных злоупотреблениях»). Так, ст. 814 ревизует ст. 1030 («Мошенничество и связанная с ним деятельность в отношении компьютеров») Титула 18 Свода законов США, и озаглавлена «Уголовно-правовое сдерживание и предупреждение кибертерроризма». Конгресс США тем самым создал новое законодательное понятие «кибертерроризм» и отнес к нему различные квалифицированные формы хакерства и нанесения ущерба защищенным компьютерным сетям граждан,

МЕЖДУНАРОДНАЯ КОМПАНИЯ GROUP IB ОПУБЛИКОВАЛА В 2014 ГОДУ СТАТИСТИКУ КИБЕРПРЕСТУПНОСТИ В РОССИИ: МОШЕННИЧЕСТВО В ИНТЕРНЕТ-БАНКИНГЕ, БАНКОВСКИЙ ФИШИНГ И МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

составляет

42%

ОТ ВСЕХ ОСТАЛЬНЫХ ПРЕСТУПЛЕНИЙ КОМПЬЮТЕРНОЙ НАПРАВЛЕННОСТИ В СТРАНЕ

юридических лиц и государственных ведомств, включая ущерб медицинскому оборудованию, «физический вред какому-либо лицу», «угрозу общественному здоровью или безопасности», «ущерб, причиненный компьютерной системе, используемой государственным учреждением при отправлении правосудия, организации национальной обороны или обеспечении национальной безопасности» (ст. 814 нового закона). Понятие «кибертерроризм» включает уголовно наказуемые деяния, хакерские посягательства, наносящие материальный ущерб на совокупную сумму от 5 тыс. долл. и выше (ст. 814), и наказываемые крупными штрафами или наказанием в виде лишения свободы от пяти до двадцати лет.

Этот параграф еще больше ужесточает уголовное наказание за компьютерные преступления. В случае, если злоумышленник проникает в компьютерные сети инфраструктуры США телевизионные сети, энергосети, транспортные каналы связи, системы управления водоснабжением, газификации, защищенные абонентские компьютеры уголовное наказание по таким видам преступлений всегда максимальное и осужденный может быть приговорен к 30 годам заключения без права досрочного освобождения. А один из разделов этого закона посвящен компьютерному шпионажу и предусматривает уголовное наказание за хищение интеллектуальной собственности американских компаний. В этом разделе установленные ранее сроки заключения для приговоренных судом по таким обвинениям увеличиваются с 15 до 20 лет.

Если проанализировать динамику законодательного противодействия федеральных органов США киберпреступности в целом, то можно обратить внимание, что не реже одного раза в два года их формы и методы претерпевают модернизацию в сторону ужесточения наказания. Таким образом, правоохранительная система США если и не опережает, то, по крайней мере, находится на равных позициях с преступниками, находясь при этом в более серьезной весовой категории. Возникает закономерный вопрос: что мешает российскому законодателю хотя бы присмотреться к этим законодательным инициативам и действующим федеральным актам американских коллег?

Международная компания Group IB опубликовала в 2014 году статистику киберпреступности в России: мошенничество в интернет-банкинге, банковский фишинг и мошенничество с банковскими картами составляет 42 % от всех остальных преступлений компьютерной направленности в стране. По данным всероссийского опроса предпринимателей, проведенного в ноябре 2017 г. Аналитическим центром НАФИ, потери от кибератак в стране оцениваются в 115 967 204 788 рублей. В период с 2018 по 2020 г. федеральный бюджет потратит 1,59 млрд руб. на реализацию мероприятий в рамках развертывания Государственной системы обнаружения предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), этим проектом занимается ФСБ. Но давайте посмотрим на российскую проблему киберпреступности не с точки зрения организации противодействия данной группе преступлений с помощью федеральных силовых структур, коммерческих экспертных организаций и посредством колоссального финансового вливания денежных средств из государственного бюджета, а с точки зрения недопущения вообще каких бы то ни было благоприятных условий для развития этой преступной тенденции. Не лучше ли потратить бюджетные средства не на сдерживание и противодействие, а на создание такого правового инструмента, который просто не давал бы мошенникам шансов совершать эти преступления. Задуматься о реализации таких форм и методов цивилизованного развития информационно-финансовой среды, в которой просто не было бы места для преступных групп кибернаутов.

Разумеется, можно проводить бесконечное обучение сотрудников силовых ведомств, вкладывать колоссальные бюджетные деньги на борьбу с киберугрозами, тратить время и ресурсы на выявление и расследование подобных преступлений, постоянно быть готовыми к отражению атак, но факты – вещь упрямая, улучшений на этом фронте борьбы в ближайшей перспективе аналитиками IT рынка не прогнозируется. Вот тут и приходит понимание той карательной стратегии, которая была сформулирована еще в 80-х годах прошлого века зарубежными специалистами, которые в то время не могли себе даже представить с каким угрожающим размахом и глубиной проникновения коберпреступности во все сферы жизни человечества придется столкнуться мировому сообществу сегодня. ●