КАК ПОБОРОТЬ СИСТЕМУ

Задача правоохранительных органов — не только ловить мошенников и наказывать их за уже совершенные преступления, но и проводить активную профилактику действий злоумышленников. Заместитель начальника 11-го отдела Главного управления уголовного розыска МВД России Владислав Парамонов считает, что устранить причину, саму возможность, при которой мошенники могут завладеть деньгами наших граждан и организаций, гораздо легче и дешевле, чем потом раскрывать эти хищения.

Современные страховые технологии: Как Вы оцениваете уровень преступности, связанный с использованием цифровых технологий?

Владислав Парамонов: Деятельность предприятий, учреждений, организаций неуклонно переходит в онлайн, в том числе с цифровыми технологиями активно работает банковский и страховой сектор. Последние три года мы особенно тщательно проводим анализ преступлений, связанных с информационными и телекоммуникационными технологиями (далее — ИТТ). В статистические сборники МВД России были внесены соответствующие дополнения.

За этот период мы видим рост преступлений, связанных с цифровой сферой. Но в 2021 году этот рост несколько приостановился. По хищениям денежных средств, кражам с электронных кошельков граждан статистика показывает даже небольшое улучшение: показатель снизился на 9,6 %. Наши эксперты говорят, что возможно достигнут уже некий пик роста IT-хищений.

Появление удобных для клиента способов использования цифровых инструментов всегда сопряжено с риском возникновения новых методов и средств осуществления хищений. До последнего времени при проектировании сервисов мало внимания уделялось изучению возможности использования их не только легитимными пользователями, но и злоумышленниками.

МВД России предпринимает определенные шаги, чтобы устранить причины

преступности, то есть закрыть те организационно-технические и правовые лазейки, благодаря которым преступники могут покушаться на финансовые активы граждан и организаций. Участники рынка, госрегулятор (Банк России) и отраслевые сообщества также принимают меры по недопущению возможности мошеннических операций. Это называется организацией антифродных мер.

ССТ: Чтобы противостоять преступникам, необходима определенная техническая подготовка работников правоохраны. Какие мероприятия проводятся в этом направлении?

В. П.: В структуре МВД в конце 2019 года были созданы специализированные подразделения по борьбе с преступлениями, совершенными с использованием ИТТ на федеральном и региональном уровне. Они есть внутри подразделений следствия, внутри уголовного розыска, внутри антинаркотических подразделений и т. д. Созданные в уголовном розыске, следствии, дознании специализированные подразделения по ИТТ постепенно увеличивают эффективность своей работы: повышается квалификация сотрудников, нарабатываются методики раскрытия и расследования IT-хищений, улучшается взаимодействие с участниками информационного обмена.

В статистике противоправных действий, совершенных с использованием цифровых технологий, распоряжением Генеральной прокуратуры выделено несколько десятков составов преступлений: против личности, половой неприкосновенности, связанных с наркотиками, с хищением имущества и денежных средств и т. д., включая непосредственно преступления в сфере компьютерных технологий. Зачастую речь идет о многогранном воздействии на психику людей. Эта преступность не знает ни границ, ни территорий, ни региональных особенностей. Цель одна — с помощью современнейших средств телекоммуникаций обмануть человека и завладеть его деньгами.

Владислав Парамонов

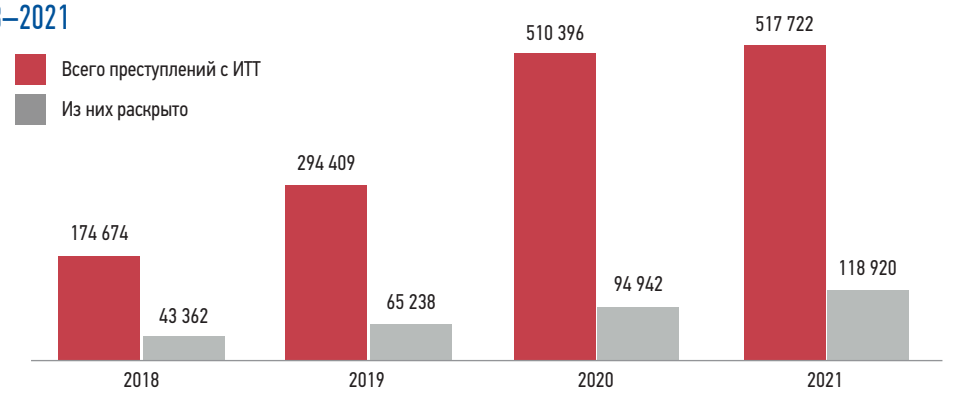
Заместитель начальника 11-го отдела Главного управления уголовного розыска МВД России

ССТ: Преступления в киберпространстве — это всегда действия организованных групп?

В. П.: В одиночку эти преступления обычно не совершают, ведь почти всегда требуется некоторая инфраструктура. Кто-то вкладывает в этот бизнес деньги, закупает оборудование. Организованная группа может располагаться не только на территории России, но и, например, в ряде стран бывшего советского пространства. Существуют целые учебные центры, которые готовят «звонарей» и иной персонал. С ними занимаются психологи, специалисты по лингвистическому программированию. Таким образом, все большее и большее количество ранее законопослушных людей втягивается в преступную деятельность.

Отдельно существует сфера вывода похищенных денежных средств в реальную денежную среду. При этом бизнес, связанный с обналом, тоже трансформировался. Деньги часто выводятся на банковские карты, оформленные на совершенно других граждан. Вот такая серьезная преступная

Количество зарегистрированных и раскрытых преступлений, совершенных с использованием ИТТ. 2018–2021



инфраструктура выросла на почве использования современных цифровых технологий. А использование криптовалют еще больше усугубило ситуацию.

Когда преступный кол-центр находится вне территории Российской Федерации, работа по его изобличению строится в рамках заключенных международных договоров, конвенции об оказании правовой помощи. Мы систематически проводим встречи с представителями полиции иностранных государств. Механизмы сотрудничества есть, но, к сожалению, не со всеми странами они эффективно работают.

ССТ: Как бороться с этой махиной?

В. П.: В одиночку МВД здесь трудно справиться. И нам уже помогают и Минцифры, и операторы связи, и банковские и страховые учреждения. Для финансовых организаций это репутационные риски, и они очень заинтересованы в том, чтобы их клиенты чувствовали себя спокойно. У многих банков сформирована мощная система — антифрод. Многие подозрительные операции уже блокируются самой финансовой организацией. Но есть и те, кто про антифрод практически не думают.

В поле зрения нашего нового специализированного подразделения попала группа в мессенджере «Telegram», которую злоумышленники создали для совершения хищений денежных средств с банковских счетов граждан посредством использования сайтов «Avito.ru» и «Youla.ru».

Суть схемы такова: что будущую жертву, разместившую объявление на «Avito», злоумышленники плавно переводили на общение в «ВатсАпп», куда и присылали поддельную ссылку о якобы «безопасной сделке». Созданная «хакерами» ссылка позволяла тайно похищать в пользу участников организованной группы денежные средства.

Администратор, он же организатор, разработал план и механизм совершения хищений, а также алгоритм действий ее участников, который опубликовал в публичном доступе. Все вступившие в группу и желающие заработать по умолчанию давали «молчаливое» согласие на совершение преступлений таким способом.

Администратор также предоставлял виртуальные абонентские номера, VPN (средство для шифрования выхода в сеть Интернет), возможность вывода денежных средств.

Все участники конференции были зарегистрированы в общем чате конференции (группе) под вымышленными никнеймами (именами) и со скрытым номером телефона. После совершения противоправных деяний участник группы получал 70% денежных средств, остальное делили организаторы.

Вывод денежных средств осуществлялся с помощью онлайн-сайтов «виртуальных» валют, а затем на банковские карты и электронные кошельки. Регистрация на криптообменнике осуществлялась автоматически по никнейму в чат-боте криптообменника мессенджера «Telegram».

При использовании этой схемы особую тревогу вызывает возможность вовлечения в преступную деятельность неограниченного числа лиц, возможно ранее не совершавших никаких преступлений!

Принимая во внимание международный и межрегиональный характер преступлений (66 субъектов РФ), учитывая необходимость проведения большого объёма следственных действий и оперативно-розыскных мероприятий, сформирована следственная группа. В ходе проведения оперативно-розыскных мероприятий оперативными сотрудниками установлены организатор и администратор.

Выявлено 2474 никнейма, по которым через криптообменник установлены банковские карты и электронные кошельки, используемые для легализации похищенных денежных средств.

На сегодняшний день установлено около 1 тыс. лиц из 67 субъектов Российской Федерации, состоящих в конференциях (группах), совершающих уголовно-наказуемые деяния.

Приведенный пример показывает, насколько многогранна правоохранительная деятельность в сфере ИТТ, сколько усилий приходится прилагать, чтобы выявить и изобличить всех преступников, сколькими новыми знаниями должны овладеть опер и следователь для успешного изобличения преступников.

> Когда преступный кол-центр находится вне территории Российской Федерации, работа по его изобличению строится в рамках заключенных международных договоров, конвенции об оказании правовой помощи.

ССТ: Как усилить профилактические меры по предотвращению мошеннических действий?

В. П.: Изобретательность мошенников часто превосходит самые смелые предположения. Когда создается какой-то новый электронный сервис, его разрабатывают не мошенники — поэтому они не могут представить, каким образом их разработка может быть использована в преступных целях. Но уже сейчас финансовым организациям стоит задуматься, как тестировать свое ПО, свои сервисы на возможность их применения в схемах киберпреступлений. Представляется, что такая экспертиза не является задачей правоохранительных органов. Хотя, может быть, со временем будет что-то меняться, и могут быть созданы дополнительные специализированные подразделения для такого тестирования.

ССТ: В конце прошлого года появилась новая схема мошенничества в ОСАГО, построенная на рассылке SMS с предложением перезаключить договор на новый срок. При этом мошенники пользуются базами данных ГИБДД и РСА, применяют продвинутые программные средства для имитации обращения к публичным базам от имени физических лиц. Есть ли возможность пресечь подобную практику?

В. П.: В центральном аппарате МВД с этой схемой пока не сталкивались, но меня ваш рассказ не удивляет. Преступные группировки имеют в своем составе и продвинутых технарей, кто пишет программное обеспечение или роботов, и специалистов в области страхования. Если мошенническая схема «пошла», злоумышленники могут ее продавать даже по франшизе.

Но чтобы могла подключиться правоохрана, в каждом конкретном случае пострадавший должен сам написать заявление

в компетентные органы. Потерпевшим, согласно УПК РФ, признается конкретный гражданин, который заплатил за полис не страховой компании, а мошеннику. В МВД России созданы специальные базы зафиксированных преступлений, позволяющие сравнивать между собой информацию из заявлений и выявлять какие-то общие черты, идентифицировать группы преступников.

ПРИМЕР РАСКРЫТИЯ КИБЕРПРЕСТУПЛЕНИЙ. САНКТ-ПЕТЕРБУРГ

В апреле 2021 сотрудники ГУУР МВД России, ГУ МВД России по Санкт-Петербургу и Ленинградской области в Москве и Санкт-Петербурге задержали 12 членов устойчивой группы, которые представлялись сотрудниками службы безопасности банков, использовали методы социальной инженерии и похищали денежные средства со счетов граждан. По местам проживания фигурантов и их связей проведены обыски, в результате которых изъяты 20 флеш-накопителей, 32 сотовых телефона, 57 банковских карт, 5 sim-карт, 6 ноутбуков, 6 планшетов, 4 жестких диска, 4 внешних диска, плеер, моноблок, машинка для счета денег, детектор купюр, денежные средства в сумме более 14 млн руб.

ССТ: Но ведь мошенничество может быть вскрыто, только когда в дорожно-транспортном происшествии выяснится, что у человека недействительный страховой полис. То есть через месяц или через год, а то и никогда. Получается, преступление останется безнаказанным?

В. П.: Если автовладельцы будут в своей массе иметь фальшивые полисы ОСАГО, то это чревато огромной социальной проблемой. Чтобы сработать на опережение, Союзу страховщиков нужно обратиться к нам, и тогда мы можем совместно продумать схему борьбы.

Если РСА известны конкретные потерпевшие, мы просим дать им рекомендации о том, чтобы они обязательно обратились в правоохранительные органы по указанному факту. И страховщики тоже должны сейчас превентивно дать своим клиентам информацию о том, что такие схемы мошенничества существуют и что обязательно необходимо обращаться с заявлениями в МВД. Застрахованные лица должны знать о том, что нельзя доверять вот таким SMS. Возможно, страховщикам нужно разработать единый формат информирования клиента о пролонгации договора ОСАГО, чтобы все прочие форматы было легко идентифицировать как подложные.

Также нужны определенные действия и от страховщика, и от страхового союза, чтобы направлять клиента для оплаты страховки только на определенные сайты и по определенным реквизитам и т. д. Возможно, потребуется наладить дополнительный контроль со стороны страховой компании. Например, перед списанием денег со счета страхователя эту операцию должен подтвердить непосредственно сотрудник страховщика. Эти меры тем более актуальны, что сейчас расширяется тарифный коридор ОСАГО. Для кого-то полис может стать дороже, и мошенники захотят воспользоваться желанием человека сэкономить и будут усиливать свое воздействие на людей.

ССТ: Какие еще конкретные шаги МВД России и страховое сообщество могут предпринять для противодействия и профилактики возникновения подобных схем?

В. П.: Нам нужно побороть систему со стороны государства. Такое мошенничество ставит под вопрос защищенность граждан: они думают, что у них есть страховая защита, на самом деле не будучи застрахованными.

Первый шаг — какими-то аппаратно-программными средствами со стороны страховщиков на корню пресечь возможность мошенников использовать данные по полисам ОСАГО. Второй — реагирование по тем заявлениям, которые уже поданы от граждан. Третье — это изобличить мошенников и дать их действиям правовую оценку. Это комбинированная профилактика.

Возможно, нужно максимально облегчить форму обращения в правоохранительные органы для человека в случае выявления мошеннических действий. Например, сделать так, чтобы заявление заполнялось на сайте страховщика и оттуда направлялось в МВД. Потерпевшим при определенных обстоятельствах может быть признана организация: если деньги не пришли в страховую компанию, фактически, у страховщика украли страховую премию, и он может обратиться к нам с соответствующим заявлением. К тому же мошенничество очень вредит репутации страхового бизнеса.

Человек должен не только чувствовать себя защищенным, он должен быть защищенным на практике. Если не бороться с мошенничеством в одной сфере, например, в ОСАГО, то дальше оно распространится на тему жизни и здоровья и так далее. Этого нельзя допускать. Социальная значимость страхования накладывает большую ответственность на все наши действия.

ССТ: Какие планы у МВД по преодолению преступлений в цифровой сфере на этот год?

В. П.: У нас большие планы по расширению электронного взаимодействия со всеми организациями — участниками рынка финансовых услуг. Мы стараемся создать некий инструмент для сокращения времени в системе «вопрос-ответ» для получения информации в электронном виде. Требуются определенные изменения в законодательстве, и эти инициативы также будут реализовываться в этом году.

Также у нас большая программа по повышению квалификации тех сотрудников, которые задействованы на этом поле битвы с преступностью. Мы проводим учебные сборы, семинары. Курсы повышения квалификации для работников МВД организованы по всей стране и охватывают все звенья как на уровне субъектов РФ, так и на федеральном уровне.

Мы проводим большую работу по формированию грамотности населения в части «цифровой гигиены» и противодействия мошенникам. Уже готовится ряд короткометражных фильмов по наиболее распространенным сегодня преступлениям, построенным на социальной инженерии, когда жертва вводится в такое когнитивное состояние, что абсолютно доверяет и исполняет указание преступника.

Кстати, на сайтах многих крупных банков уже появились разделы для потребителя, которые дают информацию, как не попасться на удочку мошенника. Есть практика, когда банки предоставляют своим клиентам антивирусные программы, чтобы обезопасить их ПО от вредоносного воздействия мошенников: их выкладывают на сайте или совершенно бесплатно направляют при открытии счета. Неплохо было бы, если бы аналогичные сервисы и информационные разделы появились на сайтах страховщиков и страховых союзов. Такая конструктивная техническая помощь клиентам помогает не допустить, чтобы злоумышленники забирали деньги наших граждан и организаций. Устранить возможность преступления всегда легче и дешевле, чем потом гоняться по всему миру за мошенниками.