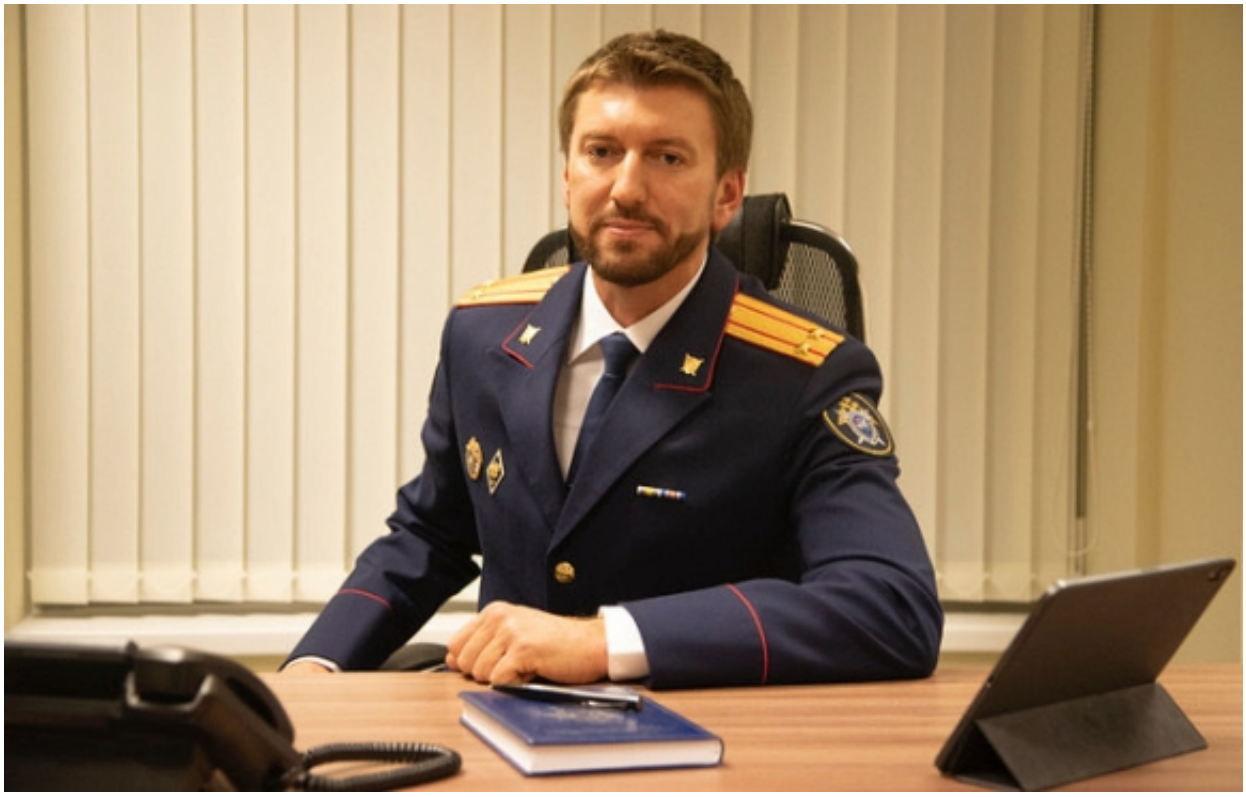
Интервью руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России Константина Комарды ИА "ТАСС"



СК: для решения проблемы "слива" баз данных в Сеть нужен новый законодательный подход

Почти год в Следственном комитете России работает новый отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий. Его руководитель Константин Комарда рассказал в интервью ТАСС о проблемах "слитых" в даркнет баз данных россиян, сложностях расследования уголовных дел с использованием криптовалюты и о том, зачем понадобилось создавать этот отдел.

— Константин Павлович, чем обусловлена необходимость создания такого отдела в СК? Количество киберпреступлений растет настолько, что другие структуры уже не

справляются с этим массивом дел?

— Создание специализированного подразделения по борьбе с киберпреступностью было вызвано объективными причинами — научно-техническим прогрессом, расширением информационной сферы и степени влияния интернета на жизнь практически любого человека. Новые технологии не только привносят в нашу жизнь комфорт, но и являются источниками новых вызовов.

Киберпреступность — это следствие всеобъемлющей цифровизации современного общества, требующее принятия адекватного противодействия со стороны государства. Она посягает на совершенно разные сферы жизни и общества — имущественные права граждан, объекты критической инфраструктуры, права личности, причиняют ущерб коммерческим организациям и государству в целом. При этом действия киберпреступников становятся все более агрессивными, они принимают меры к тщательному сокрытию следов, сохранению анонимности, продумывают свое поведение так, чтобы максимально осложнить сбор доказательств и избежать ответственности. Эти обстоятельства предопределяют правовую и фактическую сложность доказывания по таким делам. Практически всегда при совершении киберпреступлений применяются методы цифровой конспирации: шифрование данных, в том числе с использованием специализированных программ для маскировки IP-адресов, выход в Сеть через публичные точки доступа, использование учетных записей и идентифицирующих данных, принадлежащих иным лицам, не осведомленным о таком использовании, и так далее.

В целом с 2013 года уровень преступности в сфере информационных технологий возрос более чем в 20 раз и продолжает увеличиваться. Сегодня каждое седьмое преступление в России совершается с помощью информационных технологий или в киберпространстве

Традиционные подходы к расследованию преступлений не позволяют в полной мере противостоять этому качественно новому виду угроз. Необходимым условием успешной работы в этом направлении является понимание сотрудниками правоохранительных органов специфики функционирования киберсферы, ее трансграничного характера, умение работать в информационной среде, коммуницировать с представителями IT-компаний и другими специалистами, знать, как и где искать доказательства, как их фиксировать. И в конце концов грамотно построить диалог с участниками уголовного процесса, допросить свидетелей, подозреваемых и обвиняемых в совершении таких преступлений.

— Основной массив преступлений в сфере компьютерной информации относится к подследственности МВД. Какие составы преступлений будет расследовать новый отдел СК?

— Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, совершаются не только в сфере компьютерной информации (например, создание, использование и распространение вредоносных компьютерных программ, неправомерный

доступ к компьютерной информации и так далее), но и зачастую являются преступлениями общеуголовной направленности, посягают на половую неприкосновенность несовершеннолетних, могут носить террористический или экстремистский характер, преследовать цель хищения денежных средств граждан и организаций, причинять ущерб бюджетной системе государства. Эти составы преступлений отнесены к компетенции СК России.

— Сейчас остро стоит проблема продажи "слитых" в даркнет различных баз данных россиян. В частности, недавно было опубликовано журналистское расследование о том, как их используют мошеннические кол-центры, похищающие деньги под видом сотрудников банков. Вы будете подключаться к расследованию таких случаев?

— Вопрос незаконного использования личных данных граждан действительно очень актуален. В Сеть утекают сведения о паролях от личных кабинетов, данные банковских карт, о счетах и остатках денежных средств на них, паспортах, номерах мобильных телефонов и так далее. Причины этого явления разнообразны. Согласно исследованию Международного союза электросвязи, в 40 из 84 стран меньше половины населения обладает базовыми навыками работы с компьютером. Низкий уровень компьютерной грамотности населения является благоприятной средой для деятельности злоумышленников. Добавить к этому недостаточное принятие мер компаниями по защите от внутренних и внешних киберугроз, ошибки в работе сотрудников, производящих утечки информации либо умышленное хищение баз данных, — и сведения о миллионах наших граждан оказываются в Глобальной сети.

Необходимо понимать, что человек может и не подозревать об утечке его данных, а зная об этом — принять меры к их оперативному блокированию. Все дело в том, что такие сведения в открытом доступе не встретишь — они продаются на специальных ресурсах, например, в даркнете, куда простому человеку не попасть. Это уже неоднократно продемонстрировали материалы наших расследований, когда "слитые" в Сеть персональные данные использовались для подготовки и совершения особо тяжких преступлений. Для решения этой проблемы нужен комплексный подход, в том числе на законодательном уровне. Следственный комитет участвует в этой работе в рамках своей компетенции.

— В МВД и ФСБ уже давно функционируют отделы по борьбе с киберпреступностью. По каким направлениям вы сотрудничаете?

— Мы сотрудничаем с оперативными подразделениями МВД и ФСБ, которые специализируются на информационной преступности. Безусловно, у нас проводятся совместные мероприятия, в частности, коллеги оказывают помощь путем проведения оперативных мероприятий по расследуемым делам.

— Одним из условий работы в вашем отделе вы назвали необходимую

квалификацию в IT-сфере. Опыт каких стран и структур вы используете?

— Профессия следователя в принципе предполагает постоянное повышение квалификации и самообучение. Использование зарубежного опыта по борьбе с киберпреступностью является одним из условий профессионального роста сотрудников отдела, и мы работаем в этом направлении. В декабре прошлого года состоялась российско-французская встреча по проблемам противодействия киберпреступности. Со стороны Франции принимали участие прокуроры из суда общей юрисдикции Парижа, руководитель отдела по борьбе с киберпреступностью, следователи Центрального управления по борьбе с преступностью, связанной с информационными и коммуникационными технологиями, сотрудники полиции. Мы обменивались опытом следственной работы, обсуждали практические вопросы поиска и фиксации доказательств, проблемные моменты в области правоохранительного сотрудничества и способы их возможного решения.

— Вы сказали о трансграничном характере киберпреступности. Контактируете ли вы с зарубежными коллегами в данной области?

— Безусловно, международное правоохранительное сотрудничество является одним из направлений деятельности ведомства, и отдел по поручению руководства Следственного комитета принимает участие в этой работе.

По делам, находящимся в производстве, часто приходится направлять зарубежным коллегам запросы о правовой помощи, предусматривающие проведение следственных действий на их территории. Соответствующие запросы иностранных государств исполняются и в нашей стране.

Кроме того, в настоящее время производится подготовка инициированной Россией Конвенции ООН по противодействию киберпреступности. В рамках этого мероприятия проходят многочисленные консультации с представителями правоохранительных органов Евросоюза и коллегами из США. Киберпреступность в силу своего трансграничного характера — это вызов правопорядку не отдельного государства, а всему мировому сообществу. Требуется объединение усилий стран в этом направлении, выработка адекватных способов и механизмов, способных переломить сложившуюся ситуацию.

— С какими основными трудностями и проблемами сталкивается следователь при расследовании подобных дел? Удается ли их решать?

— Мы расследуем дела в отношении профессиональных злоумышленников, являющихся специалистами в сфере IT-технологий, уверенно чувствующих себя в киберсреде, тщательно планирующих преступления и использующих весь возможный арсенал средств для того, чтобы сохранить свою анонимность и остаться безнаказанными, — от VPN-программ до криптовалюты.

Например, по делам о заказных убийствах было установлено использование одной из криптовалют в качестве средства платежа. Установление источника ее происхождения, отслеживание транзакций требует тщательного подхода. Когда речь идет о конвертации криптовалюты в реальные денежные средства, преступниками используются сотни электронных кошельков, оформленных на посторонних лиц.

Транзакции производятся через 15–20 электронных кошельков, где тщательно размываются в числе десятков тысяч других операций, прежде чем попадают к конечному получателю. Это сделано для того, чтобы запутать следователей и не дать им возможности определить заказчика преступления и его соучастников

Безусловно, отследить операции, проанализировать данные, сопоставить полученные результаты без современного программного обеспечения невозможно. Поэтому мы взаимодействуем для решения этих практических вопросов с привлеченными IT-специалистами. Отрадно, что в такой непростой работе используется исключительно российское программное обеспечение.

Вместе с тем необходимо помнить, что не бывает идеальных преступлений, не оставляющих следов. И найти их — наша задача.

— Расскажите про сотрудников вашего отдела.

— Наш отдел молодой, совсем недавно ему исполнился год. За это время удалось разрешить вопрос с кадровым наполнением. Коллектив подобран из грамотных следователей, состоявшихся в качестве профессионалов, имеющих огромное желание работать в сложной, абсолютно новой и в то же время очень интересной сфере, способных искать нестандартные подходы для решения поставленных задач.

Беседовала ***Ксения Семеновская***

15 Января 2021

Адрес страницы: https://sledcom.ru/press/interview/item/1529946