8 июля – тематическое 5 - Михеев

Уважаемые участники конференции!
Коллеги, дамы и господа!

Рад приветствовать вас на конференции руководителей прокуратур европейских государств.

Тема настоящей сессии – противодействие киберпреступности – злободневная и актуальная, как никакая другая.

Вчера на открытии конференции Генеральный прокурор Российской Федерации И.В. Краснов отметил взрывной рост киберпреступности во всём мире. Она стала настоящим вызовом мировому порядку, и эта проблема особенно обострилась на фоне пандемии коронавируса.

Действительно, информационные технологии развиваются столь стремительно, что проникают во все сферы общественной жизни. Уже привычными становятся расчеты криптовалютой, использование цифровых активов, искусственного интеллекта. Однако правовое регулирование явно не успевает подстроиться к новым реалиям.

Этим, к сожалению, пользуются злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

О том, как противодействовать киберпреступлениям, не знающим ни границ, ни юрисдикций, мы сегодня и поговорим.

И начнем с нашего уважаемого гостя из Совета Европы, заместителя председателя Комитета Конвенции о киберпреступности Педро Верделью.

Прошу Вас, господин Верделью.

***

(выступление П. Вердельо, предоставление слова Генеральному прокурору Словении Д. Шкете и Федеральному прокурору Бельгии Ф. Ван Леуву).

***

Благодарю Вас, господин Ван Леув, за очень интересное выступление.

Теперь, коллеги, позвольте поделиться российской практикой и российскими подходами к вопросам противодействия киберпреступности.

В России число преступлений, совершенных с использованием информационно-коммуникационных технологий, возросло до масштабов, позволяющих говорить о них как об угрозе национальной безопасности. Если ещё пять лет назад лет назад в общей структуре преступности на долю таких деяний приходилось менее 2 %, то сейчас это **каждое четвертое** преступление, зарегистрированное в стране.

По итогам прошлого года число таких деяний достигло 510 тыс. За год увеличение составило 70 %, что, конечно же, не может не вызывать серьезную обеспокоенность.

Новые технологии всё чаще применяются для совершения самого широкого круга преступлений.

Например, рост незаконного оборота наркотиков сопровождается увеличением фактов их бесконтактного сбыта, когда реализация запрещенных веществ происходит в обмен на криптовалюту. Полученные преступные доходы отмываются и вновь попадают в криминальный оборот, используются для финансирования организованной преступности, терроризма, незаконных массовых акций.

Самые распространенные деяния этой категории – кражи и мошенничества, при этом очень часто для их совершения используются методы социальной инженерии или фишинга.

Обобщение информации о лже-сайтах свидетельствует о том, что преступники умело встраиваются в новостную повестку. Многие ресурсы связаны с торговлей лекарствами, вакцинацией, выплатами социальных пособий. Осуществляется активная рассылка фишинговых писем, предлагающих прострой и быстрый способ заработка, в том числе связанного с оборотом криптовалюты. Отмечен прирост сайтов-клонов известных торговых площадок, мошеннических предложений при онлайн-продажах.

Самые вредоносные рассылки стали более таргетированными и потому чаще вызывают доверие у получателей.

Особую тревогу вызывает использование возможностей ИКТ в **террористических целях**, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников.

За 5 месяцев текущего года из более 1 тыс. выявленных преступлений террористического характера 25 % совершено с использованием сети «Интернет».

Удельный вес **экстремистских** деяний, совершенных в Интернете, еще выше и составляет 66 % от их общего числа (320 из 484).

К последним тенденциям преступности стоит отнести размещение экстремистского контента на личных страницах в социальных сетях и мессенджерах.

Дело в том, что создание и информационное наполнение тематических сайтов постепенно утрачивает целесообразность, так как это связано с арендой доменных имен, необходимостью постоянного администрирования веб-ресурсов. К тому же их проще идентифицировать и ограничить к ним доступ. Создание зеркал тематических сайтов также не обеспечивает их сохранность, так как их обнаружение и блокировка не требуют вынесения новых решений судами и органами власти.

В целом в Российской Федерации функционирует достаточно эффективная система пресечения распространения информации противоправного характера в сети «Интернет». Роскомнадзором ведется 2 реестра противоправной информации, наполнение которых в части экстремистского и террористического контента обеспечивается органами прокуратуры.

Первый реестр формируется на основании решений судов по искам прокуроров о признании информации запрещенной к распространению на территории России ввиду наличия признаков экстремизма. Ежегодно прокурорами в суды общей юрисдикции направляются заявления о признании запрещенными порядка 5 тыс. интернет-страниц. После попадания в реестр обеспечивается их блокировка. Это, в частности, материалы, оправдывающие и пропагандирующие идеи терроризма и экстремизма.

Второй реестр формируется на основании требований Генеральной прокуратуры Российской Федерации об ограничении доступа к информации в сети «Интернет» во внесудебном порядке. Это могут быть в том числе материалы, содержащие призывы к осуществлению террористической деятельности. Ежегодно Генеральным прокурором или его заместителем принимается порядка 300 решений о внесудебном ограничении доступа к информации.

***

Чем же, коллеги, обусловлены столь широкое распространение киберпреступлений и в то же время их высокая латентность?

Существует целый **комплекс причин**. Среди них – трансформация способов шифрования данных, максимально повышающих анонимность злоумышленников, отсутствие непосредственного контакта с потерпевшим, охват широкой

аудитории, простота доступа к информации и, конечно же, **трансграничный характер деяний, совершаемых в цифровой среде.**

Отсюда закономерно вытекает следующий вопрос: что с этим делать? **Как эффективно бороться с киберпреступностью?**

С учетом тех обстоятельств, которые мной обозначены, очевидно, на национальном уровне с этим не справится ни один отдельно взятый государственный орган, также как и на международном уровне этого не сделает ни одно отдельно взятое государство.

Действовать и внутри станы, и за рубежом нужно сообща, единым фронтом. И вот эту самую функцию **координации** деятельности государственных органов в области противодействия информационной преступности в нашей стране выполняет Генеральная прокуратура Российской Федерации.

Хотел бы отменить, что с приходом Игоря Викторовича Краснова в качестве руководителя надзорного ведомства проблемам киберпреступности стало уделяться особое внимание.

В июле прошлого года этот вопрос под его председательством обсужден на Координационном совещании руководителей правоохранительных органов Российской Федерации.

По итогам этого мероприятия был решен целый ряд организационных задач, выработаны согласованные с иными ведомствами меры, такие как:

разработка единых критериев отнесения преступлений к совершенным с использованием информационно-коммуникационных технологий;

проведение анализа положений национального законодательства для его совершенствования;

планирование дополнительных проверочных мероприятий, например, по пресечению фактов незаконной реализации сим-карт;

определение проблем во взаимодействии следственных и оперативно-розыскных подразделений.

Уже сейчас можно говорить о положительных примерах скоординированной нами работы.

Так, результатом осуществленного правоохранительными органами комплекса оперативно-розыскных мероприятий и следственных действий, проведенных практически синхронно в 62 точках, расположенных в 11 субъектах Российской Федерации, стало задержание 30 активных членов и руководителей хакерской ОПГ. В итоге ОПГ прекратила свое существование вместе с почти сотней интернет-магазинов, предназначенных для оборота запрещенных предметов.

Кроме того, ведется работа по активизации инструментов государственно-частного партнерства, поскольку ключевое значение для эффективного противодействия киберпреступлениям имеет качество взаимодействия с организациями, располагающими оперативно значимой информацией. Речь идет о банках, операторах связи, владельцах интернет-сервисов, центрах реагирования на компьютерные инциденты и об организациях сферы кибербезопасности.

Вместе с тем мы можем сколь угодно совершенствовать методы противодействия киберпреступности, но до тех пор, пока люди будут сообщать мошенникам свои платежные данные, хищения будут продолжаться.

Именно поэтому Генеральная прокуратура активно участвует в процессах профилактики рассматриваемых преступлений, в том числе путем правового просвещения через официальный аккаунт в социальных сетях.

В то же время, коллеги, для принятия эффективных скоординированных мер недостаточно проведения только одного координационного совещания, путь и столь масштабного по спектру затронутых проблем.

Именно поэтому было принято решение о создании под эгидой Генеральной прокуратуры межведомственной рабочей группы по противодействию информационной преступности.

Этот постоянно действующий орган образован в июле прошлого года для решения оперативных задач в рассматриваемой сфере.

Помимо традиционных участников координационной деятельности – правоохранительных органов, группа также включает представителей МИДа России и Минюста России, поскольку своей задачей видит не только проработку национальных вопросов, касающихся повышения эффективности работы правоохранительных органов в борьбе с киберпреступностью, но и выработку консолидированной российской позиции по этой теме на международной арене, в том числе в работе специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Наша практика международного сотрудничества, в том числе оказания правовой помощи по уголовным делам о киберпреступлениях, свидетельствует о крайне низкой эффективности действующих механизмов, в результате чего выигрывают только преступники, а правоохранители (как российские, так и иностранные) оказываются не у дел.

Проблемы и в разных подходах к криминализации деяний, и в сложных процедурах, искусственно увеличивающих сроки рассмотрения запросов о правовой

помощи, и в неурегулированности многих аспектов в действующих международных договорах.

Поэтому с точки зрения основного правоприменителя считаем крайне важной и актуальной выработку на площадке ООН единого всеобъемлющего универсального инструмента, регламентирующего сотрудничество государств в борьбе с киберпресутпностью.

Рассчитываем здесь на помощь всех государств. Хочется надеяться, что совместными усилиями нам удастся сделать новый шаг на пути укрепления взаимопонимания и сотрудничества в очень сложной и исключительно важной области противодействия преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий.

***

В то же время, коллеги, мы понимаем, что это процесс небыстрый. Согласование текста глобальной конвенции и её открытие для подписания займут не один год.

Поэтому мы параллельно двигаемся по пути укрепления двусторонней базы сотрудничества.

Прежде всего, речь идет о межправительственных соглашениях, работа над которыми ведется МИДом России.

Кроме того, Федеральным законом Генеральная прокуратура наделена полномочиями по осуществлению прямых связей с компетентными органами других государств и международными организациями, в том числе по заключению с ними межведомственных соглашений и иных договоренностей.

Этими полномочиями мы активно пользуемся. К настоящему времени у нас более 90 соглашений с иностранными партнерами. За последний год заключено 4 из них: с генеральными прокуратурами Бразилии, Португалии, Белиза и Армении. При этом в каждом из 4 соглашений вопросы взаимодействия в области

противодействия киберпреступлениям поставлены во главу угла. Эти вопросы мы также включаем в программы сотрудничества с министерствами юстиции и прокуратурами зарубежных государств, разрабатываемые на краткосрочный период – обычно 2-3 года.

Кроме того, в декабре прошлого года тема противодействия киберпреступности стала ключевой на встрече руководителей прокурорских служб стран БРИКС, проведенной под нашим председательством. Подписан итоговый документ, определивший рамки международного взаимодействия.

Таким образом, убежден, что только сочетание национальных и международных мер при общих подходах всех заинтересованных субъектов способно привести к прорывному результату в противодействии информационной преступности. Наша задача – дать миру уверенность в том, что любой виновный в компьютерном преступлении будет оперативно установлен и справедливо привлечен ответственности в любой юрисдикции.

Благодарю за внимание!