Выступление эксперта Генеральной прокуратуры Российской Федерации Н.Гудкова в ходе VI заседания Межправительственной группы экспертов по киберпреступности по пункту 3 «Предупреждение преступности»

Уважаемые коллеги!

Современный этап развития общества характеризуется возрастающей ролью технологических процессов в киберпространстве.

По мере все более широкого распространения в повседневной жизни электронных устройств и систем подключения к глобальным сетям увеличиваются посягательства, совершенные с использованием Интернета и коммуникационных устройств, которые всё чаще выступают средством совершения самого широкого круга преступлений.

Помимо хищений денежных средств с расчётных пластиковых карт и электронных счетов, все большую актуальность приобретают посягательства в киберпространстве на общественную безопасность, бизнес и государство, при этом не редко в этих целях используется шантаж, информационные блокады и другие методы компьютерного давления, компьютерного шпионажа и передачи информации лицам, не имеющим к ним доступа.

Причем с каждым днём появляются новые способы шифрования данных, максимально повышающие анонимность совершаемых действий. Наблюдается широкое распространение криминального использования криптовалют в сфере незаконного оборота наркотиков, коррупции, финансирования организованной преступности, экстремизма и терроризма.

Именно поэтому уже сейчас важно объеденить усилия для скорейшей выработки под эгидой ООН новой единой универсальной Конвенции о сотрудничестве в сфере противодействия информационной преступности.

Что касается вопросов борьбы с киберпреступлениями на национальном уровне, то для их решения на площадке Генеральной прокуратуры функционирует соответствующая межведомственная группа, в которую входят не только представители правоохранительного блока, но и всех заинтересованных ведомств.

Кроме того, данные вопросы в очередной раз были рассмотрены на координационном совещании. По его итогам разработан комплекс мер, направленных на построение системы способной не только противодействовать уже совершенным киберпреступлениям, но также предупреждать и прогнозировать их.

В частности, запланированы мероприятия по повышению квалификации всех категорий лиц, осуществляющих функции по противодействию преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий, а также комплексному развитию системы экспертного сопровождения данных действий.

Кроме того, планируется наладить более тесное взаимодействие с центрами реагирования на компьютерные инциденты и организациями сферы кибербезопасности.

Безусловно, в этой связи также предстоит работа и по дальнейшему совершенствованию законодательства, которое ежегодно пополняется соответствующими нормами по мере появления новых вызовов.

Также планируется расширить возможности существующих автоматизированных поисковых систем, интегрировав их с программами искусственного интеллекта.

Однако уже сейчас эта работа весьма эффективна. С начала года удалено порядка 30 тысяч материалов суицидальной направленности и детской порнографии, свыше 8 тысяч материалов пронаркотического характера и 50 тысяч материалов пропаганды экстремизма, терроризма, а также иная запрещенная к обороту информация.

Продолжена разработка мероприятий в сфере оперативно-розыскной деятельности, с акцентом на пресечение деятельности организованных преступных групп.

Положительным примером межведомственного взаимодействия по пресечению преступной деятельности является реализованный в марте текущего года комплекс скоординированных правоохранителями страны по времени

оперативно-розыскных мероприятий и следственных действий в 62 адресах в 11 субъектах Российской Федерации, итогом которых стало задержание 30 активных членов и руководителей хакерской ОПГ. В результате совместных мероприятий ОПГ прекратило свое существование, включая функционирование более 90 интернет-магазинов, объединённых в единую информационную систему, предназначенную для приобретения, хранения и сбыта электронных средств платежей.

И такие примеры в последние годы далеко не редкость.

Ну и конечно же особое внимание будет уделено международному сотрудничеству, в частности более эффективному использованию возможностей специализированных сетей правоохранительных органов, международного полицейского взаимодействия и договоров.

Подобные инструменты существуют и сегодня, однако развитие технологий требует от нас соответствующего движения по совершенствованию механизмов взаимного сотрудничества.

Тем более, что проблем в этом направлении все еще не мало. Примером тому служит длительное неисполнение наших запросов по уголовным делам о ложных сообщениях о готовящихся в прошлом году взрывах на нескольких сотнях объектов социальной инфраструктуры в различных регионах страны, с использованием сервиса анонимной электронной почти «Мэйлфэнс».

Кроме того, мы можем сколь угодно совершенствовать методы противодействия киберпреступности, но до тех пор, пока люди сами будут сообщать мошенникам свои платёжные данные, хищения будут продолжаться.

В этой связи Российская Федерация активно участвует в процессах профилактики рассматриваемых преступлений. В первую очередь, через официальные сайты государственных органов и иных учреждений. Например, аккаунт Банка России в социальных сетях, имея среднемесячную посещаемость в размере 260 тысяч человек, ведет активную деятельность по разъяснению необходимых мер финансовой и информационной безопасности.

Достаточно серьёзный опыт в области повышения уровня киберграмотности населения Российская Федерация демонстрирует на международном уровне.

Примером может служить недавний международный онлайн тренинг по киберпреступности (Cyber Poligon), аудитория которого составила более 5 млн человек по всему миру.

В качестве рекомендаций полагал бы возможным предусмотреть:

- создание автоматизированных информационных комплексов фиксирующих весь объем данных по преступлениям, совершенным в сфере информационно-коммуникационных технологий;

- формирование централизованных ведомств по борьбе с такими преступлениями;

- совершенствование технических и экспертных возможностей противодействия высокотехнологическим преступлениям;

- формирование единых стандартов в сфере международного сотрудничества на основе современных угроз в рамках единой универсальной Конвенции под эгидой ООН.

В заключение хотел бы отметить, что мы готовы к выработке таких мер, которые позволили бы эффективно отвечать на вызовы в киберпространстве, при сохранении баланса по защите прав человека в информационной среде.

Только совместными усилиями мы сможем минимизировать криминальную активность в информационно-¬коммуникационной сфере на международном уровне.

Благодарю за внимание!

Unofficial translation

Statement by N. Gudkov, Expert from the Prosecutor General's Office of the Russian Federation, at the 6th Session of the Intergovernmental Expert Group on Cybercrime under Item 3 *Prevention of Crime*

Dear colleagues,

The current phase of society development is characterized by the increasing role of technological processes in cyberspace.

As electronic devices and systems for connecting to global networks become increasingly common in everyday life, Internet and communication gadgets are increasingly being used in attempts to commit a wide range of crimes.

In addition to theft of funds from plastic cards and electronic accounts, cyberspace infringements on public security, business and the State are becoming increasingly important, and blackmail, information blockades and other methods of computer pressure, computer espionage and transmission of information to unauthorized persons are not uncommon.

Every day, new methods of data encryption also emerge, maximizing the anonymity of the actions taken. There is a wide spread of criminal use of cryptocurrencies in connection with drug trafficking, corruption, organized crime, extremism and terrorism financing.

That is why it is currently important to join efforts to develop as soon as possible a new universal convention on cooperation in combating cybercrime under the auspices of the UN.

With regard to issues related to combating cybercrime at the national level, a relevant interdepartmental group, which includes not only representatives of the law enforcement sector but also of all the interested departments, is operating on the platform of the Prosecutor General's Office in order to resolve them.

Moreover, those issues were once again addressed at the coordination meeting. As a result, a set of measures was developed aimed at building a system

capable not only of countering the cybercrime already committed, but also of preventing and predicting it.

In particular, measures will be taken to provide advanced training to all categories of persons who are engaged in countering crimes committed with the use of modern information and communication technologies, as well as to ensure comprehensive development of a system of supporting these actions with expertise.

Moreover, it is planned to establish closer collaboration with computer incident response centres and cybersecurity organizations.

Naturally, there is also work to be done in this regard to further improve legislation, which is updated annually when relevant norms are being incorporated as new challenges emerge.

There are also plans to expand the capabilities of the existing automated search engines by integrating them with artificial intelligence programmes.

However, this work is already highly effective. Since the beginning of 2020, about 30,000 materials of suicidal nature and containing child pornography, more than 8,000 materials promoting drug abuse and 50,000 materials containing propaganda of extremism, terrorism, and also other information forbidden to circulation have been removed.

There are ongoing efforts to develop inquiry and investigative measures with a focus on curbing the activities of organized criminal groups.

A positive example of interdepartmental cooperation to suppress criminal activity is a range of time-coordinated inquiry and investigation activities undertaken in March 2020 by the country's law enforcement departments in 62 locations in 11 constituent entities of the Russian Federation, which made it possible to detain 30 active members and leaders of a hacker OCG. As a result of joint measures, the OCG has ceased to exist, including the operation of more than 90 online shops integrated into a single information system designed to purchase, store and sell electronic means of payment.

And such examples have not been uncommon in recent years.

Naturally, special attention will also be paid to international cooperation, in particular to a more effective use of the capabilities of specialized networks of law enforcement agencies, international police interaction and treaties.

Similar tools exist today as well, but the development of technology requires us to act accordingly towards improving mechanisms for mutual cooperation.

All the more so because there are still quite many problems in that area. An example of this is the longstanding failure to comply with our requests in criminal cases of false reports of explosions prepared last year at several hundreds of social infrastructure facilities in various regions of the country, with the use of the Mailfence anonymous e-mail service.

Moreover, we can endlessly improve our methods to counter cybercrime, but as long as people themselves tell their payment details to fraudsters, thefts will continue.

In this regard, the Russian Federation actively participates in the processes of preventing these crimes. First and foremost, it is done through official websites of the State bodies and other institutions. For example, the Bank of Russia account in social networks, visited by 260,000 people during an average month, is active in explaining the necessary financial and information security measures.

The Russian Federation is demonstrating a rather considerable experience in raising the level of cyber-literacy among the population at the international level.

An example of this is the recent international online training on cybercrime (Cyber Poligon), with an audience of over 5 million people worldwide.

As recommendations, I would consider it possible to envisage the following:

- creation of automated information complexes containing the entire volume of data on crimes committed in the ICT-related field;
- creation of centralized departments to combat such crimes;
- improvement of technical and expert capabilities to counter high-tech crimes;

- elaboration of unified standards in the field of international cooperation proceeding from modern threats within the framework of the single universal convention under the UN auspices.

In conclusion, I would like to note that we are ready to develop measures that would allow us to respond effectively to the challenges in cyberspace, while maintaining a balance in protecting human rights in the information environment.

It is only through joint efforts that we will be able to minimize criminal activity in the ICT-related sphere at the international level.

Thank you!