Выступление эксперта Следственного комитета Российской Федерации Т.Салихова в ходе VI заседания Межправительственной группы экспертов по киберпреступности по пункту 3 «Предупреждение преступности»

Добрый день!

Хотел бы сфокусировать внимание на теме, вызывающей у Следственного комитета России высокий профессиональный интерес, а именно на преступлениях, совершаемых против несовершенолетних.

Среди множества проблем, связанных с их безопасностью в Глобальной сети, я бы особенно выделил рост онлайн-груминга и развращения детей.

В упрощенном виде типичное преступление происходит следующим образом: преступник, выдающий себя за несовершенолетнего, регистрируется на различных Интернет площадках, вступает с ними в переписку, склоняет к фотографированию и видеосъёмке в обнаженном виде. В дальнейшем преступник часто шантажирует таким контентом несовершеннолетнего, угрожая распространить материалы среди его знакомых, вынуждает присылать больше контента. Последствия таких преступлений ужасны и подразумевают различные психологические травмы и риски совершения суицидов.

Об одном из расследуемых нами сейчас аналогичных преступлений стало известно потому, что преступник исполнил угрозы и создал фейковый аккаунт с интимными фотографиями ребенка, отказавшегося присылать ему новые. Преступник выманил фотографии у 48 детей, а пытался выманить у 324. Лишь несколько родителей, вступили в переписку с педофилом, но никто из них не сообщил в правоохранительные органы.

Ранее уже отмечали, что участие частного сектора способно существенно улучшить безопасность в Интернете. Я с этим соглашусь.

Посещая общественные места, например такие как торговые центры, мы понимаем, что они достаточно безопасны и строились с соблюдением различных норм. Установлена пожарная сигнализация, есть запасной выход,

камеры видеонаблюдения. А в случаях, когда обнаружен преступник, то охрана попробует его задержать и сообщить правоохранительным органам.

Вызывает удивление, что популярные Интернет-площадки не придерживаются схожих правил, хотя они часто знают о противоправной или сомнительной деятельности пользователей, получая такую информацию через механизмы обратной связи. На мой взгляд, такие площадки должны выстраивать свою архитектуру учитывая не только риски взлома и защиты персональных данных, но и риски использования их продуктов педофилами, а в явных случаях обращать внимание правоохранителей.

Схожих методов придерживаются некоторые рекламные площадки и банки, которые используя средства автоматизированного контроля и механизмы обратной связи выявляют подозрительную (аномальную) активность, помечают и блокируют аккаунты, а затем сообщают правоохранительным органам о преступной деятельности.

Таким образом, помимо общих рекомендаций по формированию у детей механизмов критической оценки получаемых сведений, постоянной работе по распространению правил безопасного поведения в Интернет и повышению родительского контроля, считаю необходимым обсудить вопрос о выработке дополнительных международных норм по защите детей, предъявляемых к онлайн-платформам, используемым для общения и знакомств.

Полагаем, что такие механизмы должны дополнять концепцию «security by design», т.е. безопасность детей должна стать неотъемлемой частью системы, ее нужно интегрировать во все компоненты, в обязательном порядке рассматривать все потенциальные угрозы и внедрять зарекомендовавшие себя решения.

Unofficial translation

Statement by T.Salikhov, Expert of the Investigative Committee of the Russian Federation, at the 6th Session of the Intergovernmental Expert Group on Cybercrime under Item 3 *Prevention of Crime*

Good afternoon!

I would like to focus on a topic of keen professional interest to the Investigative Committee of Russia, namely crimes committed against minors.

Among so many problems related to their safety and security on the World Wide Web, I would single out the growth of online grooming and corruption of children.

In summary, a typical crime occurs as follows: an offender, passing himself/herself off as a minor, registers at various websites, enters into correspondence with others, and inclines them to take nude pictures or make nude videos. Afterwards the offender often blackmails a minor with such content, threatening to distribute this material among his/her acquaintances, and forces him/her to send more content. The consequences of such crimes are terrible and involve various psychological traumas and suicide risks.

One of similar crimes we are investigating now has come to light because the offender carried out his threats and created a fake account with intimate pictures of a child who had refused to send him any new ones. The offender got pictures out of 48 children and tried to do the same with 324 others. Only a few parents entered into correspondence with the pedophile, but none of them reported this to law enforcement agencies.

We have noted earlier that private sector involvement can significantly improve internet security. I would agree with that.

When visiting public places, such as shopping malls, we know that they are safe enough and that they were constructed according to various standards. They have fire alarm system installed, emergency exit, and CCTV cameras. And in cases

where an offender is detected, security will try to apprehend him/her and report this to law enforcement agencies.

It is surprising that popular websites fail to follow similar rules, although they are often aware of illegal or dubious activity pursued by users since they receive such information through feedback mechanisms. In my opinion, such sites should build their architecture taking into account not only personal data hacking or protection risks, but also the risk of their products being used by pedophiles, and in clear-cut cases, bring this to the attention of law enforcement officers.

Similar methods are adopted by some advertising platforms and banks which use automated controls and feedback mechanisms to identify suspicious (abnormal) activity, mark and block accounts, and then report criminal activity to law enforcement agencies.

Therefore, in addition to general recommendations, such as to develop skills allowing children to critically assess the information they receive, to constantly work on the dissemination of rules of safe behavior on the internet and improvement of parental control, I believe it necessary to discuss elaborating additional international standards on child protection, required for online platforms that are used for communication and dating.

We believe that such mechanisms should complement the concept of "security by design", i.e. children's safety and security should become an integral part of the system, it should be integrated into all its components, with all potential threats considered and proven solutions implemented.