Тезисы выступления старшего прокурора отдела 36 управления Генеральной прокуратуры Российской Федерации Курдюкова А.Н.
(г. Санкт-Петербург, 05 июня 2018 г.)

Уважаемые коллеги!

Я рад предоставленной возможности выступить сегодня перед данной аудиторией и благодарен за это организаторам нашей встречи.

Несомненно, что развитие информационных технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. К сожалению, этим пользуются не только добросовестные пользователи коммуникационных сетей, но злоумышленники, преследующие различные противоправные цели - личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост преступлений, совершаемых с использованием современных информационно-коммуникационных технологий.

Такая динамика преступности диктует необходимость повышения эффективности противодействия киберпреступности, что бесспорно относится к стратегическим направлениям деятельности правоохранительных органов. И одной из важнейших задач в этом случае является совершенствование действующего законодательства, в целях усиления защиты граждан и общества от преступных посягательств. Уголовно-правовые запреты должны отвечать

существующим реалиям и в полной мере обеспечивать соразмерную ответственность за совершение преступных посягательств. При этом в случае динамично развивающихся видов преступности, что особенно актуально для киберпространства, конструкция уголовно правовых норм должна не просто учитывать складывающуюся кримоногенную обстановку, но и, в идеале, заглядывать в будущее, предсказывая в своей фабуле возможные опасные варианты развития методов и средств применения информационно-коммуникационных технологий в противоправных целях.

Например, в целях борьбы с компьютерной преступностью Уголовным кодексом Российской Федерации предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния как: неправомерный доступ к охраняемой законом компьютерной информации независимо от способа его совершения, создание, использование и распространение вредоносных компьютерных программ; мошенничество в сфере компьютерной информации, а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Кроме того, совершение преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») рассматривается в целом ряде составов Уголовного кодекса Российской Федерации в качестве квалифицирующего или отягчающего наказание признака – ч. 3 ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки,

телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 228.1 (п. «б» ч. 2, ч. 3, 4, 5) «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» и другие.

Поэтому можно с уверенностью сказать, что действующими уголовно-правовыми запретами охватываются основные варианты противоправных деяний в рассматриваемой сфере.

Более того правоохранительными органами осуществляется работа по обеспечению законодательной защиты новых объектов посягательств в киберпространстве, появление которых обусловлено стремительным развитием информационных технологий.

В частности, с 01.01.2018 вступили в силу изменения уголовного закона, устанавливающие ответственность за неправомерный доступ к критической информационной структуре Российской Федерации, а также за создание и распространение компьютерных программ предназначенных для этих целей (статья $274^1$ УК РФ).

Несомненно, что использование вредоносных компьютерных программ в корыстных целях превращает криминальную деятельность в сверхдоходную. Существующие правила эксплуатации сети Интернет обеспечивают анонимность преступных действий и возможность доступа к значительным материальным ресурсам.

В связи с чем угроза стать жертвами этих деяний в современных условиях распространяется на всех участников информационно-телекоммуникационной сферы, включая владельцев банковских дебетовых карт и мобильных телефонов.

Однако далеко не всегда кибер-преступления совершаются с использованием специальных познаний. Следует признать, что большинство преступлений в рассматриваемой сфере совершается с использованием методов «социальной инженерии», то есть несанкционированного доступа к информации или системам хранения информации без использования технических средств. Технология основана на использовании слабостей человеческого фактора и, к сожалению, является достаточно эффективной. Злоумышленник получает информацию, например, путем сбора информации о объекте атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего. Преступник также может позвонить человеку, являющемуся пользователем кредитной карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковском счетом, зачастую дезинформируя о его блокировке. И очень часто этот трюк срабатывает.

По сути известный присутствующим фишинг — тоже техника «социальной инженерии», направленная на жульническое получение конфиденциальной информации. Обычно злоумышленник посылает цели e-mail, подделанный под официальное письмо — от банка или

платёжной системы — требующее «проверки» определённой информации, или совершения определённых действий. Это письмо обычно содержит ссылку на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести конфиденциальную информацию — от домашнего адреса до пин-кода банковской карты.

Социальная инженерия также используется для распространения троянских коней: эксплуатируется любопытство, либо алчность цели. Злоумышленник отправляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа.

Такая техника остаётся эффективной, поскольку многие пользователи не раздумывая кликают по любым вложениям или гиперссылкам.

Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, что увеличивает риски оказаться жертвой мошенников.

Учитывая данное обстоятельство, а также то, что в Российской Федерации борьба с преступностью рассматривается как комплексное явление, включающее в себя не только поиск виновных, привлечение

их к ответственности, но и меры, направленные на предупреждение преступлений, по итогам состоявшегося 23 сентября 2016 года совещания руководителей правоохранительных органов, принято решение о проведении правоохранительными органами среди населения правового просвещения, направленного на разъяснение широким слоям населения основ информационной безопасности.

Говоря о социально уязвимых группах нельзя не отметить, что очень часто сеть «Интернет» используется злоумышленниками в отношении несовершеннолетних и молодежи. И речь идет не только об распространении порнографических материалов с их участием.

С развитием информационных технологий и глобальной сети «Интернет» несовершеннолетние активно общаются посредством социальных сетей, которые в свою очередь стали одним из инструментов и способов совершения преступлений. Стремительное распространение информации в сети не всегда позволяет оперативно отслеживать безопасность общения.

Органами прокуратуры Российской Федерации выявляются многочисленные интернет-сайты, содержащие призывы к совершению суицидов, детальное описание механизмов причинения вреда здоровью и фотографии с демонстрацией способов совершения самоубийства.

Ряд совершенных несовершеннолетними в прошлом году суицидов связан с деятельностью так называемых «групп смерти», в сети «Интернет», что вызвало широкий общественный резонанс и повлекло уголовное преследование создателей таких сообществ.

Названные группы, имеющие наименования «Синий кит», «Тихий дом» и иные, предлагают подросткам вступить в игру, длящуюся 50 дней, имеющую несколько уровней. Их преодоление возможно при условии успешного прохождения подростками 50 заданий, среди которых причинение себе резаных ран на руках и иные действия, причиняющие вред здоровью и жизни ребенка. При виртуальном общении на несовершеннолетнего оказывается психологическое давление, для облегчения выполнения заданий его убеждают в ненужности, отсутствии любви близких, соответственно бессмысленности жизни. После этого вовлеченный в «игру» подросток должен совершить суицид.

С целью предотвращения таких инцидентов и исключения возможности доступа несовершеннолетних к информации суицидальной направленности и иной запрещенной законом, создан Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, содержащих сведения, распространение которых в Российской Федерации запрещено.

Генеральная прокуратура Российской Федерации принимает активное участие в выявлении такой информации и осуществлению ее блокировки, во взаимодействии как с уполномоченными государственными органами, так и администрацией различных сетевых ресурсов.

Кроме того, упомянутые события послужили основанием введения с 07.06.2017 в Уголовный кодекс Российской Федерации статьи предусматривающей ответственность за склонение к совершению

самоубийства, в том числе с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

***

В целом имеющиеся данные не оставляют сомнений в том, что преступность очень быстро приспосабливается к меняющимся условиям. И очевидно, что преступники будут расширять свою деятельность в рамках глобальной виртуальной криминальной сети, не знающей ни границ, ни юрисдикции.

А в силу возможности анонимизации в Интернете, расследование таких преступлений процесс сложный и зачастую не быстрый.

Наиболее сложные уголовные дела обычно связаны с крупными преступными группами, которые занимаются целевыми атаками, кражами денег через интернет-банк или мобильные приложения финансовых организаций. Преступники в этих случаях уделяют большое внимание тому, как скрыть свою личность — используют несколько цепочек серверов для доступа к ресурсам, применяют шифрование, постоянно переписывают программы для атак. К сожалению, зачастую по единственному инциденту установить злоумышленников в этом случае не удается. Только по нескольким эпизодам набирается материал, с которым можно работать, но даже тогда процесс поиска может затянуться. Длительное время, учитывая специфику киберпреступлений, обычно требуется, и чтобы собрать доказательную базу.

Другую сложность представляет то, что в таких преступных группах роли четко распределены и дробятся, поэтому преступление от начала до конца совершается разными людьми. Лидер группы нанимает исполнителей

определённых задач: настроить сервер, написать и распространить вредоносную программу, обеспечить защиту вредоносного софта от антивирусов и брандмауэров.

Причем такими людьми могут оказаться и обыкновенные студенты, интересующиеся информационными технологиями и иногда даже не подозревающие, что участвуют в преступной группе. Как правило, с человеком связывается аноним и предлагает деньги за определённую работу, например создание программы, настройка  сервреа и т.п. Зачастую организатор поясняет исполнителю, для чего будет применться результатм заказанной рабты.

В то же время, к примеру, при разработке программы, перехватывающей данные, исполнитель может понимать, что она может быть использована в мошеннических целях.

Иногда такие программы приобретаются у третьих лиц и автор не информирован о том, как преступники будут ее использовать, для перехвата каких именно данных.

С другой стороны программист, пишущий для «софта» защиту от антивирусов — очевидно должен осознавать, что для легальных целей такие действия не совершаются.

Например, показательно в этом отношении раскрытое в Российской Федерации уголовное дело в отношении членов преступного сообщества, которые разработали вредоносное программное обеспечение и создали частную виртуальную сеть для получения финансовой выгоды.

Их программы позволили незаконно направлять в Центральный Банк Российской Федерации электронные файлы с реестром платежей в

различных суммах на большое количество счетов, подконтрольных злоумышленникам.

Кроме того, на приобретенные ими банковские карты перечислялись похищенные денежные средства с целью их дальнейшего обналичивания.

Подготовка к совершению данных незаконных действий заняла у преступников более года, и такая тщательность позволила им совершить хищение свыше 1,2 миллиарда рублей (20 миллионов евро).

При этом вербовка членов данной преступной организации, их дальнейшее взаимодействие и осуществление своих преступных планов осуществлялись через сеть Интернет, большинство преступников не были лично знакомы и имели место жительство в различных странах мира, никогда напрямую не контактировали.

Необходимо отметить, что сегодня все большее развитие получает рынок аренды вредоносного программного обеспечения. Настоящие программисты составляют лишь определенный процент киберпреступников. Остальные — злоумышленники, которые приобрели ту или иную программу и используют ее в корыстных целях. Причем интерфейсы многих таких программ уже почти не отличаются от офисных программ и интуитивны для освоения. Не случайно популярный сегодня вариант кибератак — внедрение вредоносного программного обеспечения в сеть в автоматическом, заскриптованном режиме, когда преступнику достаточно запустить программу и ждать результатов.

Создание или модификация таких программ под специальные задачи, обозначенные заказчиком, также является одним из видов получившего в

последнее время широкое распространение в интернет-пространстве явления, которое известно как «преступление как услуга».

За определенную плату так называемые «специалисты» совершат DDoS-атаку на указанные серверы, или предоставят ботнет для тех же целей.

Развитие информационных технологий позволяет преступникам создавать новые механизмы совершения преступных деяний, которые сложны не только для обнаружения, но и для ликвидации как самих вредоносных программ, так и их последствий. И речь здесь идет не только о печально известным всем присутствующим массовых атаках вирусов-шифровальщиков (WannaCry и другие).

Например, уникально с точки зрения способа было имевшее место в Российской Федерации преступление, связанное с хищением денежных средств из банка. С помощью вредоносной программы злоумышленники получили доступ к автоматизированному рабочему месту клиента данного банка, и доступ к каждому компьютеру внутри организации, в том числе и в филиалах. Для этого на одном компьютере в сети был запущен компьютерный червь, который работал исключительно в оперативной памяти компьютера. То есть представлял собой так называемую «бестелесную программу» (fileless). Другими словами, преступники создали контролируемую бот-сеть внутри банка, в которой пока хотя бы один зараженный компьютер будет включен, он снова и снова будет заражать машины компании.

Очевидно, что в данном случае, без принудительной одновременной остановки всей компьютерной сети банка избавиться от вредоносной

программы было невозможно. И легко представить ущерб от такой остановки.

Специфика сложности установления лиц, совершающих преступления в информационно-коммуникационных сетях, накладывает свои ограничения и при расследовании преступлений. Зачастую правоохранительные органы, осуществляя производство по уголовному делу о преступлении, совершенном группой лиц, в случае установления одного из соучастников, не стремятся немедленно задержать его, а могут продолжать фиксировать его дальнейшие действия с целью выявления и задержания остальных участников преступного сообщества.

Большое внимание в прокурорами в России уделяется вопросам возмещения ущерба, причиненного киберпреступлениями.

В Российской Федерации функционирует Федеральная служба по финансовому мониторингу (Росфинмониторинг), которая является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения,.

При этом органы расследования ориентированы на активное взаимодействие с указанной службой по вопросам предоставлению сведений о суммах, характере и периодах совершения операций (сделок) лицами, причастными к преступным деяниям.

Также в настоящее время в Российской Федерации видится перспективным полноценное использование всего ресурса действующих в государственных и частных центров реагирования на инциденты в сфере

компьютерной информации, целью которых является сбор сведений об уязвимостях жизненно важных объектов инфраструктуры.

В частности был создан подобный Центр реагирования на компьютерные инциденты в кредитно-финансовой сфере. При этом в первый год его существования удалось предотвратить хищения из российских банков на общую сумму более трех миллиардов рублей (или свыше 40 миллионов евро), а также совместно с правоохранительными органами пресечь деятельность двух организованных преступных групп, уникальных по широте своей преступной деятельности и способам совершения преступлений.

На базе указанного Центра создается центр компьютерных экспертиз, что положительно сказывается на эффективности расследования преступлений, совершаемых в рассматриваемой сфере.

Также в Российской Федерации функционируют специализированные подразделения правоохранительных органов по выявлению и расследованию киберпреступлений, уже не раз доказавшие свою эффективность в борьбе с рассматриваемыми преступными деяниями.

В то же время любые организационные и практические меры, проводимые внутри одной страны, могут быть максимально результативными только при наличии надлежащего механизма международно-правового сотрудничества. В этой связи целесообразно совершенствовать существующие процедуры в части упрощения процедуры взаимодействия, в том числе использования в этой сфере современных информационных технологий.

В связи со складывающейся ситуацией, на мой взгляд, совместные усилия правоохранительных органов в сфере международного сотрудничества необходимо сосредоточить на выработке более действенных мер, с учетом технического прогресса и возрастающей сложности изобретенных преступных схем.

К сожалению не всегда уровень такого сотрудничества и скорость обмена информацией позволяет правоохранительным органам действовать быстро и адекватно, используя весь потенциал для борьбы с преступниками.

Например, имел место случай, когда при осуществлении правоохранительными органами Российской Федерации оперативно-розыскных мероприятий, направленных на выявление лиц, совершающих преступления с использованием информационно-коммуникационных технологий в правоохранительные органы иных стран (31 государство) была направлена информация относительно 177 зарубежных пользователей сети Интернет, распространяющих противоправный контент. От правоохранительных органов зарубежных государств поступило всего два ответа.

При таких обстоятельствах весьма сложно говорить об оперативном и своевременном раскрытии преступлений и привлечении к надлежащей ответственности лиц их совершающих.

При этом Генеральная прокуратура Российской Федерации придерживается активной позиции в части развития международного сотрудничества в сфере борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. С 2015

года принято участие в 12 мероприятиях по вопросам противодействия преступлениям, совершаемым с применением информационно-коммуникационных технологий и носящим транснациональный характер.

В заключение хотел бы отметить, что новые горизонты информационных технологий уже заставляют задуматься о предстоящих сложностях в правоохранительной деятельности. Уже можно наблюдать повсеместное распространение блокчейн-технологий, не за горами внедрение квантового шифрования и стремительное развитие нейросетей. Наивно было бы предполагать, что изощренные умы не попытаются приспособить и эти достижения человеческой мысли для реализации своих корыстных противоправных целей.

Полагаю, что в условиях появления новых вызовов криминального сообщества, без малейшего сомнения использующего отсутствие границ в виртуальном пространстве, мы должны быть на шаг впереди в части международного взаимодействия и прилагать максимально возможные усилия к его совершенствованию. При этом позволю себе выразить уверенность в том, что совместными действиями мы сможем если не минимизировать преступную деятельность в киберпространстве, то, самое меньшее, не позволить злоумышленникам избежать установленной ответственности за свои действия.

Благодарю за внимание!