Ибатуллина Диана Марсовна
адъюнкт
ФГКОУ ВО «Казанский юридический институт МВД РФ»
г. Казань, Республика Татарстан

DOI 10.31483/r-112866

КИБЕРВЫМОГАТЕЛЬСТВО КАК ПРЕСТУПНАЯ ТЕНДЕНЦИЯ

Аннотация*: автором рассмотрено кибервымогательство как социальная негативная ориентация, некоторые особенности данного явления, а также общие меры противодействия.*

Ключевые слова*: преступление, собственность, кибервымогательство, информационные технологии, сетевая гигиена.*

Законодатель, а также иные органы, уполномоченные толковать отдельные вопросы реализации уголовно-правовых норм, довольно точно и объемно разрешили многие спорные вопросы, касающиеся состава вымогательства, установления признаков, содержащихся в составе преступления, а также мер уголовной ответственности.

Только в 2023 году по данным главного информационно-аналитического центра МВД России было зарегистрировано 8939 фактов вымогательства, что больше на 9,1% чем в 2022 году. К тому же ежегодная статистика свидетельствует и о том, что преступления, совершаемые с использованием информационных технологий, многократно растут. В 2023 году число таких преступлений достигло 676951 (прирост 29% с 2022 года) [1].

Однако наиболее актуальной проблемой в современных реалиях является совершение кибервымогательства. На сегодняшний день в доктрине уголовного права и уголовном законодательстве единый термин «киберпреступность» отсутствует, именно поэтому в научных исследованиях можно встретить различные подходы к определению данного негативного явления. К примеру, Матросова Л.Д. компьютерное вымогательство относит к разновидностям мошенничества [2, с. 152]. Стяжкина С.А. считает, что термин «кибервымогательство»

следует использоваться для обозначения определенного рода преступных деяний, связанных с неправомерным воздействием на компьютерную информацию (наряду с такими понятиями, как фишинг, скриминг, киберджекинг и т. д. [3, с. 942].

На наш взгляд, под кибервымогательством следует понимать требование о передаче чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, совершенные с использованием информационных технологий.

Следует отметить, что применение для преступных целей информационных технологий привносит значительные трудности в практическую работу сотрудников правоохранительных органов, в частности, по выявлению, пресечению и противодействию этому негативному опасному явлению. Это связано с рядом факторов:

1) отсутствие достаточных знаний в области информационных технологий у лиц, производящих расследование.

Общественная опасность нового вида вымогательства с использованием высоких технологий возрастает также в связи с необходимостью привлечения к его расследованию специалистов узкого профиля и применения при расследовании особых технических умений, знаний и навыков.

2) сложность в идентификации преступника, так как жертва напрямую не сталкивается с вымогателем «лицом к лицу».

Усложняется и процесс по восстановлению картины произошедшего и установлению всех обстоятельств дела, в связи с тем, что вымогатель может действовать из любой точки мира и часового пояса. В связи с развитием высоких технологий для вымогательства может быть использована информация, которая находится в широкой базе сети Интернет, обеспечивающая безграничные

возможности по ее поиску. В компьютерных сетях и разнообразных каналах передачи данных обуславливает несоизмеримо широкий круг участников взаимодействия. Поэтому использование высоких технологий повышает характер и степень общественной опасности вымогательства.

Как отмечает Третьяк И.В. преступник в момент совершения преступления может находиться в любой точке мира, что затрудняет процесс сбора информации о произошедшем [4, с. 97].

Именно поэтому в условиях широкого распространения достижений научно-технического прогресса в преступные действия от правоохранительных органов требуется непрерывное внедрение мер, которые позволят своевременно и полно изучать способы кибервымогательства. В первую очередь, изучению должны подлежать технические устройства, различное программное обеспечение и иные технические объекты (содержание файлов в личном ноутбуке, текстов переписки в сетях, электронной почты и пр.), что позволит обнаружить данные о способе совершения вымогательства, характере выдвинутой угрозы, размере вымогательства, его конечной цели и других фактах, необходимых для юридической оценки содеянного.

Помимо этого, следует и трансформировать законодательные нормы. В своем исследовании Овсюков Д.А. указывает на необходимость отдельного состава преступления, устанавливающего ответственность за вымогательство в сфере компьютерной информации [5, с. 144]. Мы считаем, что необходимо ч. 2 ст. 163 УК РФ следует дополнить пунктом «д», устанавливающим ответственность за совершение вымогательства, с использованием информационных технологий, что, в свою очередь, подчеркнет повышенную степень опасности данного преступлений.

Рассмотрим наиболее распространенные способы кибервымогательства.

1. Взлом аккаунта (личной страницы) интернет-пользователя считается самым распространенным явлением. Взлом аккаунта позволяет получить доступ к личным данным, информации о трудовой деятельности, в некоторых случаях к данным счетов и т. д.

«Классической» схемой вымогательства после взлома аккаунтов выдвижение требований о переводе денежных средств взамен на отказ от публикации фотографий «интимного характера», личных данных.

Также выражается предупреждение о том, что, если потерпевший попытается заблокировать вымогателя, отправить жалобу администраторам этой социальной сети или удалить свой профиль, неудобная информация будет отправлена автоматически. Как правило, потерпевшим от подобных действий становится близкое ранее виновному лицо, которое ранее могло участвовать в различных видеороликах или фото эротического содержания [4, с. 99].

2. Не менее распространено вымогательство, сопряженное с использованием различных специальных вредоносных программ – обладающих специализированным функционалом программ-вирусов, таких как: SocGholish, ArechClient2, NanoCore т. п.

Использование вредоносных программ, позволяющих копировать данные, могут быть квалифицированы по ст. 273 УК РФ, однако при такой квалификации не учитывается, что основная цель виновных более тяжкое деяние – это именно вымогательство денежных средств или криптовалюты. Например, DDoS-атаки (типа «отказ в обслуживании») – наиболее распространенный способ изъятия криптовалюты, направленный на вычислительную систему с целью блокирования доступа пользователей, когда вымогатели требуют уплату выкупа в криптовалюте, а в случае отказа осуществляют такие атаки. Подобные деяния согласно российскому законодательству квалифицировать по ст. 163 УК РФ как вымогательство нельзя, поскольку угроза уничтожения компьютерных систем или компьютерной информации не является признаком состава данного преступления [6, с. 18].

Вместе с тем в судебной практике встречаются такие решения, в которых требования передачи имущества под угрозой DDoS-атаки, оценивались судом в совокупности с использованием вредоносной программы (например, приговор Хорошевского районного суда города Москвы от 01.12.2014 в отношении К., осужденного по ч. 1 ст. 163, ч. 1 ст. 273, ч. 2 ст. 273 УК РФ) [7].

Очевидно, что если бы предметом вымогательства под угрозой DDoS-атаки была криптовалюта, то содеянное по духу закона должно бы быть оценено как вымогательство.

Основой противодействия кибервымогательству является именно сетевая гигиена. Не стать жертвой вымогателя достаточно просто, достаточно соблюдать ряд действий: устанавливать надежную аутентификацию, периодически менять пароли на своих технических устройствах и в социальных сетях, использовать современные антивирусы, не давать доступ к своим социальным сетям другим лицам.

Таким образом, кибервымогательство сложное и часто трансформируемое преступление, борьба с которым требует специфических мер. Для противодействия данному явлению требуется единовременное применение комплекса мер, от различных субъектов (правоохранительных органов, потерпевших, иных государственных структур). Мы считаем, что первостепенными шагами для предотвращения ежегодного прироста кибервымогательства являются: принятие п «д» ч. 2 ст. 163 УК РФ, закрепляющего квалифицированный признак «с использованием информационных технологий, выработка и постоянное совершенствование методик раскрытия и расследования кибервымогательства, а также сетевая гигиена пользователей.

Список литературы

1. Состояние преступности в Российской Федерации за 2023 г. (архивные данные) // Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/folder/101762 (дата обращения: 01.09.2024).

2. Матросова Л.Д. Системный анализ понятия средств реализации и принятия решений по совершенствованию мер защиты от вымогательства в сети Интернет / Л.Д. Матросова // Закон и право. – 2018. – №11. – С. 152. – DOI 10.24411/2073-3313-2018-10250. – EDN VLCQOU

3. Стяжкина С.А. Вопросы квалификации кибервымогательства / С.А. Стяжкина // Вестник Удмуртского университета. Серия «Экономика и право». –

2022. – №5 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/voprosy-kvalifikatsii-kibervymogatelstva (дата обращения: 01.09.2024). – DOI 10.35634/2412-9593-2022-32-5-941-947. – EDN MTQLYS

4. Третьяк И.В. Новые виды вымогательства в сети интернет / И.В. Третьяк // Вестник науки. – 2018. – №7 (7) [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/novye-vidy-vymogatelstva-v-seti-internet (дата обращения: 01.09.2024).

5. Овсюков Д.А. Использование информационно-телекоммуникационных сетей при совершении вымогательства / Д.А. Овсюков // Актуальные проблемы российского права. – 2022. – Т. 16. №2. – С. 144.

6. Долгиева М.М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты / М.М. Долгиева // Современное право. – 2018. – №11. – С. 17–19. – EDN YMBWHJ

7. Приговор Хорошевского районного суда г. Москва от 01.12.2014 года по делу №1-587/2014 г. [Электронный ресурс]. – Режим доступа: https://actofact.ru/case-77RS0031-1-587-2014-2014-10-22-2-0/ (дата обращения: 01.09.2024).