нодательства в области защиты прав жертв преступлений. Тем не менее именно с момента принятия рассмотренных выше декларации и других международно-правовых норм и принципов был заложен прочный фундамент основных понятий и терминов, определены направления уголовной политики международного сообщества в целях защиты жертв преступлений, что нашло свое отражение во многих нормах уголовного законодательства государств.

На региональном уровне в 1983 г. Советом Европы была принята Европейская конвенция о возмещении ущерба жертвам насильственных преступлений. Именно эта конвенция стала результатом более глубокого осознания необходимости обеспечения баланса правового положения правонарушителя и потерпевшего от преступления. Впервые был определен компенсационный механизм обеспечения защиты жертвы преступления. Последующие Рекомендации Комитета министров Совета Европы № R(85)11 о положении жертвы в рамках уголовного права и уголовного процесса еще более детально акцентируют внимание на необходимости защиты жертв преступлений от физического, психологического, материального и социального ущерба.

В 2011 г. Советом Европы в Стамбуле (Турция) была принята Конвенция Совета Европы о предотвращении и борьбе с насилием в отношении женщин и домашним насилием. Данное соглашение определяет не столько основы защиты потерпевших, но и акцентирует внимание на необходимости предотвращения любого вида насилия. Тем не менее для многих государств стали неприемлемыми определенные положения Конвенции, в которых усматривается вероятность размытых формулировок некоторых понятий, в том числе понятие «гендер» и другие. Именно поэтому многие государства не спешат присоединяться к Конвенции, а Турция, несмотря на то, что первой подписала и ратифицировала ее, первой же из нее вышла.

Таким образом, рассмотренные международно-правовые стандарты и нормы в области защиты жертв преступлений являются фундаментом по созданию эффективных принципов и норм на региональном и внутригосударственном уровне. Именно они определяют обязанность государств обеспечивать эффективную защиту жертв преступлений, предоставлять эффективные средства национальной внутригосударственной правовой защиты потерпевшим в случае совершения преступлений, предупреждать совершение преступлений против личности, гарантировать возмещение ущерба потерпевшим от преступлений и др.

Шерстяных А.С.,

кандидат технических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

Популярные схемы кибермошенничества в 2022 году

Информационные технологии настолько прочно вошли в нашу повседневную жизнь, что современный человек уже не представляет себе существование без них. Мобильный банк, оплата телефоном или часами, мгновенная связь с абонентом, находящимся на другом конце земного шара, социальные сети, облачные хранилища и т.д. Это все настолько удобно и практично, что не может не привлекать внимание мошенников. Поэтому можно говорить о том, что постепенная информатизация мира привела к появлению нового вида преступников – кибермошенников.

Кибермошенничество – это один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номеров банковских счетов, паспортных данных, кодов, паролей и т.д.)[1].

[1] Что такое кибермошенничество и какая наступает за него уголовная ответственность // Сайт московской транспортной прокуратуры. URL: https://epp.genproc.gov.ru/web/mmtp/activity/legal-education/explain?item=69345532 (дата обращения: 24.02.2023).

Количество таких преступлений растет год от года. Особенно увеличилось их количество во время пандемии Covid-19, когда многие организации перевели своих сотрудников на удаленный режим работы, при этом экономическая активность в реальной жизни резко упала и переместилась в интернет-пространство.

Согласно опубликованным МВД России статистическим данным, в 2022 г. снизилось количество зарегистрированных преступлений, совершенных с использованием информационных технологий. В частности «…зарегистрировано на 29% меньше фактов мошенничества с использованием электронных средств платежа, на 22,5% – криминальных деяний в сфере компьютерной информации»[1].

Эксперты отмечают, что наибольшее количество атак на организации было организовано с помощью программ-вымогателей. «Они по-прежнему являются киберугрозой номер один, причем не только для международных корпораций, но и для российского бизнеса»[2].

Увеличение активности вымогателей специалисты связывают с небывалым ростом количества утечек данных российских компаний, выложенных в публичный доступ на форумах и в профильных Telegram-чатах. Летом 2022 года специалисты Group-IB отметили двукратный рост количества слитых баз данных по сравнению с весной (с одновременным уменьшением цены практически вдвое). Еще одна тенденция наметилась прошлым летом. Если раньше такие данные старались продать, то теперь их выкладывают в общий доступ для того, чтобы нанести репутационный или экономический ущерб бизнесу и / или клиентам.

В последнее время участились кражи конфиденциальных данных с помощью стилеров. Стилер – это вредоносное программное обеспечение, предназначенное для кражи ценных данных с зараженной машины, таких как куки-файлы, логины и пароли, скрины с рабочего стола и пр.[3]

«Вредонос» распространяется с помощью видеоролика на популярном ресурсе (YouTube, Telegram-каналы, соцсети и пр.). Злоумышленник оставляет ссылку на файлообменник, где якобы выложен предмет обсуждения (игра, «самый эффективный майнер», анкета для участия в розыгрыше и т.д.). Причем заливать вирусованный ролик вовсе не обязательно, достаточно разместить ссылку в описании, а можно разместить ее в комментариях к чужому ролику. Особенно выгодна, с точки зрения мошенников, схема с NFT-площадками. Злоумышленник подыскивает NFT-художника, попутно проверяя (с помощью открытых ресурсов) содержимое его криптокошелька. Затем он связывается с потенциальной жертвой в социальной сети или Telegram-канале и просит «оценить работы», просмотреть которые можно, перейдя по предложенной ссылке.

Телефонное мошенничество в 2022 г. также не утратило привлекательности для злоумышленников. Схемы совершенно разные: от надоевших всем звонков от «службы безопасности банка» или «правоохранительных органов», якобы расследующих подозрительные операции по карте, до выяснения обстоятельств перевода денег на Украину с вашего счета.

После проведения частичной мобилизации появилась новая схема обмана. Мошенники представляются волонтерами, которые якобы ведут списки военных – тех, кто попал в плен и погиб. Чтобы проверить судьбу мобилизованного, достаточно ввести его Ф.И.О. и дату рождения, а также оставить номер телефона для связи. Затем лжеволонтеры звонят и сообщают, что человек погиб. Предлагают помощь, чтобы вывезти тело на родину для захоронения (разумеется, не бесплатно).

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 г. // Сайт МВД России. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 24.02.2023).

[2] Киберцунами: как 2022 год изменил мир IT-преступлений в России // Известия : новостной сайт. URL: https://iz.ru/1447317/mariia-frolova/kibertcunami-kak-2022-god-izmenil-mir-it-prestuplenii-v-rossii (дата обращения: 26.02.2023).

[3] Стилеры и где они обитают // Блог компании Grour-IB. URL: https://www.group-ib.ru/ blog/stealers/ (дата обращения: 24.02.2023).

Фишинг[1] по-прежнему остается одной из излюбленных схем мошенничества в Интернете. Злоумышленники оперативно реагируют на геополитическую ситуацию в мире. На фоне массового ухода иностранных производителей и поставщиков из России количество фишинговых сайтов возросло (по оценкам специалистов) в 6 раз. Еще весной 2022 г. (к Международному женскому дню) появилось несколько десятков доменов, в названии которых фигурировало слово «доставка», например adidasdostavka.ru, louisvuittondostavka.ru. Фейковые Gucci, Chanel, Nike, Stradivarius, Mango, Zara и даже Porsche и Volvo, уходящие или уже ушедшие из страны, стали предлагать доверчивым покупателям приобрести свои товары. Еще одна популярная разновидность фишинга – фейковые розыгрыши ценных призов от имени известных компаний.

Российский хит среди кибермошенников 2022 г. – сайты, предлагавшие купить бумагу, особенно в тот период, когда были перебои с поставкой товара. В основном такой вид обмана был нацелен на мелкий и средний бизнес.

В июне 2022 г. Минцифры запустило в эксплуатацию информационную систему для мониторинга фишинговых сайтов ИС «Антифишинг»[2]. Она автоматически выявляет сайты, которые маскируются под официальные ресурсы госорганов, компаний, популярных маркетплейсов и социальных сетей. Результатом работы системы является блокирование вредоносных ресурсов, которые признаны фишинговыми на территории Российской Федерации.

В период опытной эксплуатации информационной системы «Антифишинг» за два месяца выявлено около 30 тыс. подозрительных ресурсов (органов государственной власти, онлайн-казино, поддельные сайты продажи билетов и т.д.), из них заблокировано 9 тыс. подтвержденных фишинговых веб-сайтов.

По-прежнему основным способом предотвращения такого рода преступлений является информирование населения страны с помощью различных средств массовой информации (публикации в газетах, листовки в общественных местах, новостные сюжеты и пр.) о схемах, используемых мошенниками для выманивания денег. Важно показать, что в похожих ситуациях не следует торопиться, нужно постараться найти возможность остановиться, обдумать ситуацию, может быть, обсудить с близкими людьми. Эти шаги могут предотвратить совершение кибермошенничества.

Канубриков В.А.,

кандидат юридических наук, доцент
Волгоградская академия МВД России

Трансформация уголовно-правовой ответственности за побои в российском уголовном законодательстве

В соответствии со ст. 22 Конституции РФ, дающей право на свободу и личную неприкосновенность, гарантируется неотъемлемое право каждого индивида на охрану жизни и здоровья. Соответственно, посягательства на здоровье человека имеют большую общественную опасность, при этом причинение побоев среди деяний, посягающих на здоровье человека, являются наименее исследованными с уголовно-правовой точки зрения. В настоящее время реалии складываются таким образом, что побои и истязание обладают повышенной латентностью, так как совершаются чаще всего в семейно-бытовой сфере, и их опасность как раз и кроется в том, что, казалось бы, не причинившие вреда здоровью повреждения с пугающей регулярностью приводят к совершению особо тяжких преступлений против жизни и здоровья, ведь почувство-

[1] Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей методами социальной инженерии, а также нанесение пользователям другого ущерба.

[2] ИС мониторинга фишинговых сайтов // ИС «Антифишинг» : сайт. URL: https://paf.occsirt.ru/ (дата обращения: 27.02.2023).