Кузора С.А.,

кандидат юридических наук, доцент
Владивостокский филиал Дальневосточного юридического института МВД России

Уровень развития киберпреступности – вызов современному обществу

Бурное развитие информационно-коммуникационных технологий оказывает влияние на все сферы деятельности человека. Однако, как уже это неоднократно бывало в истории, достижения науки и техники используются в преступных целях. Проведенное сравнение уровня и структуры преступности за 20 лет позволило выявить интересную закономерность – в конце XX начале XXI века наша страна захлебывалась от квартирных краж, грабежей и разбоев. В 2003 году было совершено 2 млн 756 тыс. преступлений (+9,1% относительно 2002 года), из них 1 млн 150,8 тыс. составили кражи, при этом каждая вторая кража была совершена из жилища (около 559 тыс.). Также было совершено 48,7 тыс. разбоев (10,5 тыс. в жилище), 198 тыс. грабежей (19,7 тыс. в жилище). Однако спустя 20 лет ситуация кардинально изменилась – за 2023 год в России совершено 1 млн 947,2 тыс. преступлений (снижение на 1% относительно 2022 года), из которых 3,4 тыс. – разбои, 22 тыс. – грабежи, 583 тыс. – кражи (20,5 тыс. – из жилища). Из указанного видно, что за два десятилетия уровень преступности существенно снизился, а количество краж грабежей и разбоев снизилось многократно. Однако на фоне снижения традиционных преступлений на первый план выходят новые виды преступлений, не встречавшиеся ранее – преступления с использованием информационно-телекоммуникационных технологий, которых к в 2023 году было совершено 677 тыс. (+29,7 в сравнении с 2022 годом). При этом удельный вес данной категории преступлений от общего количества всех преступлений за 2023 год вырос с 26,5% до 34,8% в сравнении с предыдущим годом[1]. Столь бурный рост преступлений с использованием информационно-телекоммуникационных технологий свидетельствует о формировании в обществе нового вида преступников, имеющих хорошее образование в IT-сфере, ведущих общепринятый образ жизни и не вызывающих подозрений у окружающих. Основными направлениями киберпреступности в настоящее время являются хищение денежных средств с банковских счетов, счетов граждан и юридических лиц, мошенничество с использованием методов социальной инженерии, блокирование (хищение) информации и вымогательство за счет возврата доступа к ней. При этом суммы похищенного впечатляют. К примеру, в конце 2023 года за разблокировку доступа к базе данных одной крупной российской компании федерального уровня, занимающейся медицинской диагностикой, преступники запросили 20 млн рублей в криптовалюте, и это только один пример, ставший достоянием общественности. К сожалению, большая часть преступлений в этой сфере скрывается от общественности, так как пострадавшие не желают огласки своих проблем. В 2023 году киберпреступники, используя только программы-вымогатели, заработали более 1 млрд долл. США, что вдвое превысило доходы предыдущего года (около 570 млн долл. США)[2]. В противостоянии с киберпреступниками в сравнении с традиционной преступностью существует ряд проблем. Исходя из складывающейся ситуации, всему силовому блоку, и в первую очередь МВД России, на плечи которого ложится основная задача по противодействию новым вызовам, требуется кардинальная трансформация. Необходим отход от традиционной схемы работы оперативных подразделений, требуется создание специализированных отделов, куда будут входить IT-специалисты, отрабатывающие в режиме 24/7 все сообщения о киберпреступлениях по субъекту. Имеющиеся в настоящее время подобные подразделения слишком малочисленны и зачастую

[1] Состояние преступности в России // МВД РФ : сайт. URL: https://мвд.рф/reports/item (дата обращения: 12.02.24).

[2] В 2023 году хакеры-вымогатели заработали рекордный 1 млрд долларов. URL: https://rg.ru/2024/02/11/v-2023-godu-hakery-vymogateli-zarabotali-rekordnyj-1-mlrd-dollarov.html (дата обращения: 12.02.24).

привлекаются к выполнению несвойственных функций. К тому же наблюдающийся массовый исход из-за низкого денежного содержания сотрудников МВД не позволяет привлечь необходимое количество специалистов. Попытка заставить отрабатывать сообщения о киберпреступлениях оперативных сотрудников районных отделов ни к чему не приводит – затягиваются сроки проверки, утрачиваются важные сведения. Для установления всех обстоятельств совершения киберпреступления необходимо привлечение специалистов в области IT-технологий, которые должны подключиться к раскрытию преступления незамедлительно. Специалист должен иметь возможность анализа подключений в сети Интернет, отслеживания адреса, с которого преступники совершили свое деяние, дистанционного обследования содержимого компьютера жертвы и преступника, отслеживание без лишних проволочек движения денежных средств по счетам, установления места их обналичивания, извлечения записи с банкоматов, возможности заблокировать средства на банковском счете с целью их дальнейшего изъятия[1].

Помимо трансформации силового блока, от государства требуется принять ряд нормативных актов для наведения порядка как в банковской сфере, так и в области предоставления услуг связи. Проблема получения информации онлайн от операторов связи, финансовых учреждений до сих пор толком не решена, хотя имеются существенные сдвиги – затягивание сроков получения сведений об оборудовании, использовавшемся при совершении преступления, пути движения средств позволяет оставаться в значительном количестве случаев безнаказанными. При этом до сих пор не решена проблема звонков с использованием подменных абонентских номеров. Законодатель обязал операторов связи отслеживать звонки в своей сети, внеся еще в 2021 году изменения в чч. 9, 10 ст. 46 Закона «О связи», включив в перечень требований к оператору связи обязанность передавать в сеть связи другого оператора связи, участвующего в установлении телефонного соединения, в неизменном виде абонентский номер или уникальный код идентификации, и требования по блокировке соединения сети связи иностранного оператора связи, если оно сопровождается нумерацией, соответствующей российской системе. С целью устранения данной проблемы в настоящее время государство в лице Главного радиочастотного центра, входящего в структуру Роскомнадзора, запустило систему «Антифрод», действие которой в 2024 году планируется распространить на все регионы страны[2]. Однако до настоящего времени SIP-телефония широко распространена на территории Российской Федерации, с ее использованием совершаются рекламные звонки, что также используют и преступники. Присутствует возможность совершения звонков на мобильные и стационарные телефоны с использованием возможностей сети Интернет, мессенджеров (WhatsApp, Telegram и пр.), где с высокой степенью вероятности система «Антифрод» не работает. Использование спутникового Интернета («Старлинк» или других аналогичных систем, уже появившихся неофициально на территории Российской Федерации) еще сильнее уводит преступников в тень, так как силовые структуры лишаются возможности отслеживать преступников по их оборудованию.

Помимо вышесказанного, необходимо ограничение на мгновенные банковские переводы за пределы РФ через обезличенные счета разных видов. Проблема требует незамедлительного разрешения, так перед преступником, кроме хищения денежных средств у жертвы, появляется необходимость получить возможность распоряжаться ими, для чего необходимо денежные средства в безналичной форме вывести в «безопасную зону», очистить и обратить в собственную пользу. Получая доступ к денежным средствам жертвы, преступники зачисляют денежные средства на обезличенный виртуальный счет в одной из платежных систем, после чего перечисляют их на криптокошельки и путем переводов по нескольким счетам выводят их из-под возможного кон-

[1] Черкасов В.С. Защита банковской и коммерческой тайны при производстве следственных действий в отношении электронных носителей информации // Проблемы правовой и технической защиты информации. 2022. № 10. С. 91.

[2] РКН и ГРЧЦ раскрыли детали о начале работы в РФ системы блокировки звонков с подменных номеров «Антифрод». URL: https://habr.com/ru/news/t/695720. (дата обращения: 02.02.24).

троля со стороны правоохранительных органов, теряющих возможность отследить путь похищенных денежных средств до конечного получателя. Это особенно актуально для преступлений, связанных с незаконным оборотом наркотических средств, что совершается путем дистанционной продажи через сеть Интернет. Фактически выявить и привлечь к уголовной ответственности организаторов такой преступной деятельности можно, только отследив движение денежных средств, а это в сложившейся ситуации практически невозможно. Росфинмониторинг предлагает установить обязанность банков и других компаний, переводящих деньги, «обеспечить неизменность и передачу в составе расчетных документов информации о получателе перевода». Если данных о получателе нет, то деньги должны быть возвращены плательщику, но это предложение блокируется «банковским лобби», которое не желает терять значительную комиссию по таким переводам.

Рост как общего количества, так и удельного веса киберпреступлений в общей структуре преступности в России в 2023 году требует незамедлительной реакции государства на данную проблему, однако пока нет оснований для улучшения обстановки в данной сфере.

Карпика А.Г.,

кандидат технических наук, доцент
Ростовский юридический институт МВД России (г. Ростов-на-Дону)

Актуальные вопросы противодействия киберпреступлениям

Киберпреступность является растущей проблемой, которая до сих пор не до конца понята исследователями или полицейским / правоохранительным сообществом. Жертвы киберпреступлений не всегда сразу сообщают о преступлениях, поскольку считают, что полиция недостаточно подготовлена к борьбе с этими преступлениями. Кроме того, имеются объективные проблемы сотрудников полиции, в том числе недостаток знаний в области выявления киберпреступлений и борьбы с киберпреступностью.

В статье рассматриваются текущие исследования, дающие всестороннее описание киберпреступности и решающие проблемы борьбы с такими преступлениями.

Общепризнанно, что киберпреступность существует, но не существует универсального определения того, что она означает. Термины «киберпреступность», «компьютерная преступность», «облачная преступность» и «злоупотребление компьютером» часто используются как взаимозаменяемые и могут относиться к любой преступной деятельности, связанной с Интернетом или компьютером. В связи с этим наиболее целесообразно любое преступное поведение с использованием сетевых технологий и Интернета называть «киберпреступностью», за исключением случаев, когда речь идет о конкретных исследованиях с использованием другой терминологии.

Признавая, что киберпреступность является глобальной проблемой, в данной статье основное внимание уделим борьбе с киберпреступностью в мире. Широко признано, что киберпреступность распространена и растет. По данным, приведенным в открытых источниках, за 2023 год годовой глобальный ущерб от киберпреступности, превышает 20 трлн долл. Произошло 1,7 млн атак с использованием программ-вымогателей. 71% организаций по всему миру стали жертвами атак программ-вымогателей.

Организованная преступность несет ответственность за 80% всех нарушений безопасности и данных. Атаки программ-вымогателей происходят каждые 10 секунд. Более 70% всех кибератак имеют финансовую мотивацию (за ними следует кража интеллектуальной собственности, а затем шпионаж).

Генеральной прокуратурой РФ на портале правовой статистики указано на рост (+29,4%) преступлений в сфере IT-технологий (ИКТ) или компьютерной информации, при этом на такие деяния (81,5 тыс.) сегодня приходится каждое из четырех регистрируемых преступлений.