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.

Наиболее распространены мошенничества (68%), совершенные с использованием сети Интернет (50,4 тыс.) или при помощи средств мобильной связи (32,8 тыс.), также на 24,5% выросло число краж с банковских счетов или в отношении электронных денежных средств граждан и организаций (25 тыс.)[1]. Столь же неутешительная статистика по росту киберпреступлений (~300%) прослеживается в отчетах правоохранителей за рубежом (Интерпол, Европол, ФБР и др.).

Этот рост киберпреступности и переход к ней в сочетании со взаимозаменяемой и зачастую запутанной терминологией привели к недавнему предположению, что приставка «кибер-» может вскоре стать излишней, поскольку почти все преступления будут связаны с технологиями. Действительно, все расследуемые серьезные и организованные преступления теперь подвергаются цифровому сокрытию и шифрованию, а Интернет используется для вербовки, преследований и спекуляции традиционными офлайн-преступлениями.

С момента своего широкого распространения несколько десятилетий назад Интернет в разной степени способствовал совершению правонарушений, которые можно характеризовать как преступления, совершенные посредством нарушения кибербезопасности, с использованием киберсредств. Такая типология аналогичным образом включает преступления, связанные с Интернетом (т.е. кибер-активностью), интернет-преступления (т.е. киберзависимые) и преступления против виртуальной личности.

Хотя эти преступления могут быть связаны с офлайновыми правонарушениями, такими как кража, кража со взломом, причинение преступного ущерба или мошенничество, киберпреступления не являются синонимами их оффлайновых аналогов и по-разному воспринимаются жертвами, преступниками и властями.

Экспоненциальный рост использования Интернета во всем мире связан с увеличением количества преступлений с использованием Интернета и облачных технологий, поскольку они обеспечивают увеличение централизованного пула жертв и новые возможности как для совершения преступлений, так и для уклонения от обнаружения и преследования. Более широкое использование технологий социальных сетей означает, что один преступник теперь может охватить большее число жертв, а затраты и уровень квалификации, необходимые для совершения киберпреступлений, снизились.

Преступные интернет-сообщества предлагают готовые пакеты вредоносного программного обеспечения (т.е. вредоносных программ), которые можно продавать неквалифицированным лицам, а обучающие материалы находятся в свободном доступе, что открывает рядовым интернет-пользователям доступ в мир киберпреступности, таким образом людям становится проще, дешевле и удобнее совершать киберпреступления, причем в более крупных масштабах[2].

Это изменение усугубляется развитием облачных технологий, что приводит к увеличению вычислительной мощности и памяти компьютеров. Предоставляя онлайн-пул общих ресурсов, облегчая доступ к готовому программному обеспечению для атак и к ресурсам обработки, таким как ботнеты, для выполнения и автоматизации, облако представляет собой онлайн-среду, в которой правонарушители могут охотиться, действовать и распределять добычу с относительной легкостью и анонимностью.

По своей природе, как общий центр обработки данных, облачные технологии увеличивают количество устройств, к которым можно получить доступ через подключение к Интернету, и, следовательно, количество возможностей для злоумышленников. Эффект облака как мультипликатора силы не только приводит к увеличению эффективности усилий преступников, но и еще больше снижает риск судебного преследования. Таким образом, Интернет и облачные вычисления предлагают целый спектр вариантов преступной деятельности: от влияния сетевого компьютера на традиционную преступность до пре-

[1] Айнутдинова К.А., Айнутдинова К.Н. Ключевые показатели и тенденции роста киберпреступности в России и за рубежом. URL: https://kpfu.ru/staff_files/F375787108/klyuchevye_pokazateli_kiberprestupnost.pdf (дата обращения: 10.02.2024).

[2] Карпика А.Г., Лемайкина С.В. Вопросы обеспечения национальной безопасности в киберпространстве // Актуальные проблемы современного российского государства и права : материалы ежегодной всероссийской научно-практической конференции. Калининград, 2022.

ступлений, которые автоматизированы и происходят полностью в виртуальной среде.

Пользователи-люди часто представляют собой самое слабое звено в компьютерной безопасности, и их слабости, в зависимости от типа киберпреступности, могут использоваться различными способами, превращая жертв в инструменты собственной виктимизации. Средства эксплуатации включают социальную инженерию и обман, манипулирование процессами принятия решений посредством предполагаемой срочности или авторитета, а также использование предсказуемых привычек, связанных с использованием веб-сайтов, паролей, загрузками и социальными или профессиональными сетями. Таким образом, жертвы могут винить себя или испытывать вину со стороны других, помимо потенциально разрушительных последствий, таких как финансовые потери или ущерб репутации и карьере.

Жертвы киберпреступлений могут страдать от долгосрочных психологических и эмоциональных последствий, включая посттравматическое стрессовое расстройство (ПТСР), с соответствующими последствиями для физического здоровья. Жертвы также могут чувствовать стыд или оскорбление ввиду вторжения в их частную жизнь или переживать разрыв отношений из-за финансовых потерь, утечки информации, сексуального вымогательства или мошенничества при использовании ресурсов знакомств.

Сексуальная эксплуатация в Интернете и торговля людьми являются другими примерами серьезных преступлений, увеличению и развитию которых способствовал Интернет, поскольку преступники могут легче получить доступ к жертвам и вербовать других правонарушителей, анонимно распространять материалы и получать доступ к гораздо большему числу потенциальных клиентов, что приводит к способствованию совершению этих преступлений.

Таким образом, можно сформулировать основные тезисы, необходимые при раскрытии и расследовании киберпреступлений.

1. Из-за ощущения анонимности и удаленности от офлайн-мира пользователи Интернета испытывают ложное чувство безопасности, а онлайн-преступники психологически, социально и физически отдаляются от своих преступлений и жертв, сталкиваются с меньшим количеством и / или менее серьезными последствиями своего поведения.

2. Жертвы киберпреступлений занижают информацию о своей виктимизации по сравнению с традиционными преступлениями, что, как предполагается, связано с предполагаемым недостатком понимания и готовности в полиции, и как жертвы, так и полиция выражают замешательство по поводу того, в какую организацию следует сообщать.

3. Обучение для повышения уровня знаний и предоставления стандартизированных ответов на сообщения о киберпреступлениях, а также более активное участие общественности и размещение обучающих материалов на большинстве посещаемых ресурсов могут помочь улучшить качество противодействия подобным преступлениям и защищенность граждан.

4. Расширение знаний о киберпреступлениях и причастных к ним лицах может также повысить готовность к расследованиям и повысить способность сопереживать жертвам и подозреваемым, чтобы получить лучшие результаты на допросе, генерировать более точные версии и выявлять соответствующие доказательства.

Шерстяных А.С.,

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

Браузерные расширения – киберугроза 2023 года

Многие из нас помнят время, когда для того, чтобы просматривать видео, слушать музыку или общаться с друзьями, требовалось специальное программное обеспечение. Сейчас для этого достаточно иметь браузер. Чем больше информации люди передают через браузер, тем более он привлекателен для мошенников. Вмешаться в работу браузера можно разными способами. Один из них – браузерные расширения.