Хасанова Лилиана Фанисовна,
преподаватель отделения права ГАПОУ
Уфимский колледж статистики, информатики
и вычислительной техники, г. Уфа

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ДИСТАНЦИОННЫМ СПОСОБОМ

Аннотация: В статье рассматриваются проблемы, вызванные повсеместным проникновением цифровых технологий, что, с одной стороны, создает значительные возможности для развития, как общества, так и государства, с другой стороны, расширяются возможности для преступного сообщества, когда оно овладевает новейшими методами совершения преступлений.

Abstract: The article examines the problems caused by the widespread penetration of digital technologies, which, on the one hand, creates significant opportunities for the development of both society and the state, on the other hand, opportunities for the criminal community to expand when it masters the latest methods of committing crimes. At the same time, formed an atmosphere, in which additional criminal dangers arise in various spheres of public life.

Ключевые слова: цифровые технологии, учтённые преступления, фондовая биржа, хакеры.

Keywords: digital technologies, recorded crimes, stock exchange, hackers.

Стремительное проникновение цифровых технологий, с одной стороны, предоставляет гигантские возможности для развития как общества, так и государства, с другой стороны, расширяет возможности для преступного сообщества, обогащая его новейшими методами совершения преступлений, формирует атмосферу, при которой создаются дополнительные криминальные опасности в различных сферах общественной жизни. Дополнительную нагрузку в этом направлении все государства почувствовали в связи с интенсивным распространением коронавируса и неизбежным в подобных условиях переходом на дистанционный режим работы. Подобная самоизоляция способствовала резкому росту общего числа преступлений, совершенных с использованием информационных технологий. Как свидетельствует официальная статистика МВД Российской Федерации, данные об основных показателях развития преступности в стране за 2020 год свидетельствуют о качественном росте подобных преступлений на фоне показателей предшествующего года.

Пресс – служба МВД России подчеркнула факт резкого роста числа преступлений, связанных с использованием информационно-телекоммуникационных технологий. Общий рост составил 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%. Именно подобный рост, как отмечается в отчете, повлиял на общий рост отрицательных показателей. Так, например, официальная статистика свидетельствует, что на подобном фоне общее число зарегистрированных в России преступлений увеличилось на 1%, тяжких и особо тяжких – на 14%.

Это происходит в то время, когда, по данным МВД, количество преступлений против личности по сравнению с прошлым годом уменьшилось на 5,1%, в том числе убийств и покушений на убийство – на 3,2%, умышленных причинений тяжкого вреда здоровью – на 6,7%.

Количество граждан, погибших от преступных посягательств, сократилось на 5,2%. Число лиц, которым причинен тяжкий вред здоровью, – на 6,9%. Из официальной отчетности складывается впечатление, что значительная часть преступного сообщества также «ушла на в режим самоизоляции». В частности, по итогам 2020 года наблюдалось уменьшение числа разбоев – на 21,7%, грабежей – на 16,2%, количества краж – на 3%, в том числе квартирных – на 22,6%, краж транспортных средств – на 27,1%.

Отчет МВД утверждает, что граждане стали чувствовать себя безопаснее в общественных местах. Резко понизились другие показатели. Например, преступлений на улицах, площадях, в парках и скверах было зарегистрировано меньше на 9,9%, в том числе грабежей – на 24,8%, краж – на 18,5%, разбойных нападений – на 23,3%.

Официальное сообщение завершается также в позитивных тонах: «В 2020 году зафиксировано снижение на 9,5% числа преступлений в семейно-бытовой сфере, в том числе на 15,8% – фактов умышленного причинения тяжкого вреда здоровью, на 13,5% – вреда средней тяжести, на 10% – легкого вреда здоровью» [1].

Общеизвестно, что показатели об учтенных преступлениях дают не всегда совпадающую с реальностью картину, так как их реальное число превышает официальную статистику. Однако, становится всё более очевидным, что с развитием информационных технологий и движением государства в направлении сплошной цифровизации всех сфер управления, а также общественной жизни, технический (цифровой) прогресс способствует трансформации также способов и возможностей для совершения преступлений, при этом резко увеличивается число подобных правонарушений.

Если рассматривать проблемы, связанные с преступлениями в сфере информационных технологий и выделить их в качестве самостоятельной группы, тогда можно выделить следующие составляющие:

- Отдельные составы 28 главы УК РФ, где групповым объектом являются отношения в сфере компьютерной информации, определены преступления, которые непосредственно посягают на указанную сферу общественных отношений.
- Преступления, где предметом независимо от статуса объекта гражданских правоотношений непосредственно выступает информация и ее носители, в частности, преступления, направленные непосредственно на нарушение режима охраняемых законом тайн, вторжения в сферу авторских и смежных прав, неправомерный оборот средств платежей, различные преступления в сфере оборота порнографии и пр.
- Противоправные действия, где объективной стороной выступают действия, направленные на искажение информации, в частности, фальсификация единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета, фальсификация финансовых документов учета и отчетности финансовой организации и др.
- Преступления, которые в той или иной степени могут включать или обязательно включают использование информационных технологий.

Говоря о четвёртой подгруппе, следует исходить из признания очевидного факта, что она включает в себя не только примеры, связанные с мошенничеством и его разновидностями, но также и ставшие уже традиционными составы преступлений против жизни и здоровья. Речь идёт о некачественном оказании медицинской помощи, когда используются телемедицинские технологии. В подобных случаях в зависимости от наступивших последствий, речь идёт о квалификации подобных деяний как причинение смерти или тяжкого вреда здоровью по неосторожности.

Говоря о действиях, когда подобные преступления уже совершены, следует помнить о том, что процесс расследования «по горячим следам», прежде всего, зависит от своевременности обращения пострадавшего в правоохранительные органы: от него потребуется первичная фиксация следов преступления.

Учреждения, работающие непосредственно с данными клиентов, оснащены системами логирования – позволяющими хранить информацию о действиях лиц, с указанием мест и адресов, с которых они заходили в сервис, какими телефонами пользовались непосредственно для доступа и другими действиями. Сохранение такой информации необходимо для того, чтобы можно было восстановить цепочку действий, например, в случае если клиент в переписке получил ссылку на фишинговый сайт, а также, если у потерпевшего запрашивали данные карты. В подобной ситуации соответствующие органы вынуждены запрашивать информацию такого рода.

Если совершенное преступление связано с хищением денежных средств, жертва должна получить выписку из своего банка с подтверждением факта перевода денежных средств, где указаны реквизиты лица, который их получил. При этом следует фиксировать контакты и непосредственное взаимодействия с преступниками. Речь в данном случае идет об адресе сайта и электронной почты, номере телефона, а также физическом адресе офиса злоумышленников. Специалисты настойчиво рекомендуют в случаях, когда мошенничество непосредственно связано с хищением денежных средств или использованием конфиденциальной банковской информации, ускоренными темпами произвести звонок обслуживающему банку и произвести блокировку карты. Если администрация банка будет своевременно информирована о факте неправомерного списания денежных средств, у банка будет больше возможностей для оказания содействия клиенту в дальнейшем.

Жертвам подобных преступлений следует помнить о том, что прямой обязанностью правоохранительных органов входят сбор и закрепление доказательств с описанием обстоятельств совершенного преступления. С другой стороны, отдельные специалисты предлагают после непосредственного обращения в правоохранительные органы предпринять и самостоятельные шаги с целью противодействовать преступникам. Одной из мер подобного пресечения является обращение к кураторам соответствующей доменной зоны (например, с целью заблокировать фишинговый сайт. Следует помнить, что в .RU и .РФ существуют своеобразные «организации быстрого реагирования» для предотвращения подобных случаев. Указанный список наличествует на официальном сайте Координационного центра доменов .RU/.РФ.

Общая картина не претерпела изменений и в прошлом году. За 2022 год злоумышленникам удалось украсть у банковских клиентов 14,1 млрд руб. Данная цифра стала рекордно высоким показателем с 2019 года. До этого периода ЦБ в статистике мошеннических операций учитывал только транзакции по картам. Сейчас в статистку входят все транзакции, проведенные с помощью электронных средств платежей.

За год объем хищений вырос на 4,29% «на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов с применением электронных средств платежа», как объясняется в сообщении ЦБ. В 2022 году банковские клиенты перевели 1,4 квадриллиона руб., годовой рост составил 39%.

На фоне роста объема украденных средств сокращается число мошеннических переводов: количество операций без согласия клиентов снизилось на 15,31% по сравнению с 2021 годом и составило 876,5 тыс. транзакций. В ЦБ отметили, что сокращение этого показателя произошло впервые за семь лет «благодаря расширению комплекса мер, которые банки принимают для противодействия мошенничеству»[2].

Проблемы проникновения цифровых технологий уже перестали удивлять возможными негативными последствиями. Сегодня трудно поразить информацией об очередном взломе хакерами закрытой системы. При этом утверждается, что больше всего могут пострадать брокеры на фондовых рынках. Сегодня большинство финансовых операций проходят посредством компьютерных алгоритмов, которые за секунду обрабатывают больше данных, чем человек способен осуществить за год. Соответственно не сравнить и скорость реагирования компьютера и человека на изменение цифрового материала. В литературе был приведен пример подобного вмешательства.

23 апреля 2013 г. сирийские хакеры взломали аккаунт официального твиттера крупнейшего американского новостного агентства – Ассошиэйтед Пресс. В 13.07. злоумышленники «запустили» по указанному каналу сообщение о состоявшейся атаке на Белый дом и ранении Президента США Барака Обамы. Алгоритмы на биржах, призванные ежесекундно следить за новостными каналами, отреагировали немедленно и стали с безумной скоростью продавать активы. Индекс Доу Джонса вошёл в режиме свободного падения и в течение 60 секунд опустился на 150 пунктов, что было равнозначно потере 136 миллиардов долларов. В 13.10. (спустя всего 3 минуты) агентство подтвердило, что данное сообщение оказалось «уткой». Алгоритмы технических «дали задний ход» и к 13.13. индекс Доу Джонса практически вернул все потери.

Однако, следует напомнить и о более зловещем событии, произошедшим на фоне компьютерного сбоя. 6 мая 2010 г. фондовая биржа в Нью Йорке испытала шок гораздо большего масштаба. За 5 минут уже упоминавшийся индекс Доу Джонса упал на 1000 пунктов, что означало потеря 1 триллиона долларов. Понадобилось более трех минут, чтобы вернуть утраченные позиции. Известный во всём мире израильский исследователь проблем развития цивилизации Юваль Ной Харари, описав данное событие, не удержался от едкого комментария: «Вот, что происходит, когда программы сверхбыстрых компьютеров фактически контролируют наши деньги. С того времени эксперты пытаются понять, что же произошло в этом «мгновенном крахе». Для них очевидно, что проблема заключается в алгоритмах, но никто не может ответить на вопрос о конкретной причине.» Харари с иронией отмечает, что «некоторые трейдеры в США уже подготовили судебные иски против компьютерных алгоритмов, ответственных за сделки. В исках отмечается, что тем самым подвергается дискриминации человек, который не поспевает за скоростью компьютеров. Заполнение подобной документации больше направлено не для того, чтобы выяснить представляет ли это угрозу правам человека, а на заполнение огромного объёма документов и значительные выплаты адвокатам» [3, 364].

В своей книге «Краткая история будущего» Харари, как и многие авторы, предрекает неизбежное исчезновение большинства представителей юридического профиля. Его слова полны пессимистической оценки: «Какова будет судьба всех этих юристов, когда изощренные поисковые алгоритмы смогут найти за день больше прецедентов, чем человек за всю жизнь? Когда простым нажатием кнопки аппарат для сканирования мозга сможет легко разоблачить ложь и обман? Сегодня даже опытные адвокаты и детективы не смогут разоблачить в мимике лица и тону голоса разоблачить двойственный характер показаний свидетеля, подозреваемого лица. Однако, когда человек говорит неправду, задействованы другие части мозга, в отличие от того, кто говорит правду». В недалёком будущем утверждает с определенной степенью злорадства Харари: «сканеры мозга могут работать почти как безошибочные детекторы лжи. И куда тогда деться миллионам адвокатов, судей, полицейских и детективов? Им следует подумать о том, чтобы вернуться в образовательные учреждения с целью овладеть знаниями и навыками новой профессии» [3, 365].

Столь пессимистическая оценка не совпадает с реалиями повседневной жизни. Куда исчезнут показания свидетелей, вещественные доказательства, все процедурные аспекты длительного и сложного пути расследования преступления? К тому же, автор сам ссылается на факты, свидетельствующие о том, к каким негативным последствиям могут привести сбои в работе компьютерной технологии.

Следует вспомнить, что ещё в далёком 1956 г. была опубликована научно-фантастическая новелла американского писателя Филипа К. Дика «Особое мнение». В ней описывались события, происходившие в обществе будущего. Здесь три мутанта, подключенные к огромной машине, предвидят все преступления еще до их совершения. Указанные «предсказатели» помогают особому подразделению полиции арестовывать подозреваемых раньше, чем они смогут совершить какое-либо реальное преступление. События, описываемые в произведении, привели в дальнейшем к закрытию подобной программы. Всех «преступников», не совершавших преступления, освободили из специальных капсул, где они должны были пребывать всё время.

Мутанты же были обеспечены всем необходимым и переселены втайне от всех на пустынный остров, где их стали окружать леса и морская вода. Здесь они предались любимому занятию – чтению книг[4].

В произведения получили отражение личные опасения автора книги – Филипа К. Дика. Писатель частности, ставит под сомнение сам факт существования взаимосвязи между силой предвидения и ограничением индивидуальной свободы.

Таким образом, не только литература, но и сама жизнь опровергают столь мрачные перспективы профессиональной деятельности сотрудников правоохранительных органов в будущем. Представляется очевидным, что в борьбе с преступностью, вооруженной новейшими технологиями, человек сможет победить, используя все свои знания и опыт практической деятельности, и, конечно же, прибегая к помощи соответствующих технических средств.

Список литературы:

1. https://newdaynews.ru/moscow/714108.html (дата обращения – 22 апреля 2021 г.)
2. https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f (дата обращения – 18 сентября 2023 г.)
3. Yuval Noah Harari. Homo Deus. A brief history of tomorrow. Vintage. London, 2018. P. 513.
4. Dick, Philip K. The Minority Report. The Minority Report and Other Stories. New York, NY: Citadel Press, 1987.