УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.23670/IRJ.2023.138.94

КИБЕРПРЕСТУПНОСТЬ КАК ГЛОБАЛЬНАЯ УГРОЗА: ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ

Научная статья

Нейберт А.Е.[1, *]

[1] Томский Государственный Университет, Томск, Российская Федерация

* Корреспондирующий автор (neybert.artur[at]mail.ru)

Аннотация

Статья посвящена вопросам противодействия киберпреступности и возникающим проблемам в этой сфере. Статья описывает трансграничный характер киберпреступности, что требует взаимодействия и совместной работы государств и международного сообщества. Автор подчеркивает наличие ряда проблем, связанных с противодействием киберпреступности, которые существуют в большинстве развитых стран. В статье описываются текущее положение дел в сфере кибербезопасности, основные направления борьбы с киберпреступниками, сложности при статистическом учете преступлений и проблемы распределения компетенций между государственными органами. Отдельно в статье указывается на сложность приоритизации борьбы с киберпреступностью наряду с другими опасными существующими явлениями.

Ключевые слова: киберпреступность, кибербезопасность, трансграничная преступность.

CYBERCRIME AS A GLOBAL THREAT: PROBLEMS OF LAW ENFORCEMENT

Research article

Neibert A.Y.[1, *]

[1] Tomsk State University, Tomsk, Russian Federation

* Corresponding author (neybert.artur[at]mail.ru)

Abstract

The article is dedicated to the issues of countering cybercrime and emerging challenges in this area. The article describes the cross-border nature of cybercrime, which requires cooperation and collaboration between states and the international community. The author emphasizes the existence of a number of problems related to countering cybercrime that exist in most developed countries. The article describes the current state of affairs in the field of cybersecurity, the main directions in the fight against cyber criminals, difficulties in statistical recording of offences and problems in the distribution of competences between government agencies. Separately, the article points out the difficulty of prioritizing the fight against cybercrime along with other dangerous existing phenomena.

Keywords: cybercrime, cybersecurity, cross-border crime.

Введение

Первые исторические события, связанные с киберпреступностью, берут свое начало с момента создания первых компьютерных сетей и одновременно с развитием персональных компьютеров. Хакеры-первопроходцы появились в Массачусетском технологическом институте (MIT) в 1960 году, а 20 ноября 1963 года о них упомянул один из студентов MIT [1]. Правда, термин был предназначен для обозначения причудливых манипуляций с компьютерами. С течением времени термин приобрел иной оттенок, связанный с нанесением ущерба информационным системам и компьютерам.

Швеция стала первой страной, где был принят закон о защите данных, получивший название «Закон о данных» 1973 года. В нем говорится, что данные должны быть защищены от любого несанкционированного доступа. США стали второй страной, где был принят закон о наказании за киберпреступность; этот закон был представлен сенатором Эйбом Рибикоффом и назван «Закон о защите федеральных компьютерных систем» 1977 года.

Термин «киберпреступность» был введен Суссманом и Хьюстоном в 1995 году. Киберпреступность не может быть описана одним определением, ее лучше всего рассматривать как совокупность действий или поведения – эти действия основаны на материальном объекте преступления и способе действия, которые затрагивают компьютерные данные или системы. Термин «киберпреступление» включает в себя противоправные действия, в которых цифровое устройство или информационная система являются либо инструментом, либо объектом, либо просто комбинацией того и другого.

Основная часть

В марте 2018 года Европол, агентство Европейского союза по сотрудничеству правоохранительных органов, объявило об аресте подозреваемого лидера киберпреступной сети, которая была нацелена на более чем 100 финансовых учреждений в более чем 40 странах, что привело к убыткам в размере более 1 миллиарда евро. Начиная с 2013 года эта организованная преступная группа использовала вредоносное ПО для кражи финансовых переводов и нарушения работы сети банкоматов финансовых систем по всему миру. Лидер группы был арестован в Испании после многолетнего расследования, координируемого Центром по борьбе с киберпреступностью Европола. Арест, проведенный испанской национальной полицией, включал поддержку Федерального бюро расследований США, правоохранительных органов в Румынии, Молдове, Беларуси, Тайване и ряда частных компаний по кибербезопасности [2]. Отдельно, в августе 2018 года, Министерство юстиции США объявило о том, что трое украинских граждан,

которые были членами преступной организации «FIN7» или «Carbanak Group», были арестованы в Польше, Германии и Испании. Им было предъявлено обвинение в развертывании вредоносного ПО Carbanak для более чем 100 американских компаний и краже более 15 миллионов записей карт клиентов [3].

Привлечение к ответственности только некоторых из виновных в этих киберпреступлениях включает в себя сотрудничество многочисленных правоохранительных органов. Это яркий пример глобального сотрудничества, необходимого для достижения прогресса в выявлении и привлечении к ответственности киберпреступников. Он также подчеркивает проблемы, стоящие перед глобальным сообществом правоохранительных органов, когда требуются годы сотрудничества, значительные ресурсы и десятки национальных и международных организаций, чтобы повлиять только на один элемент одной организации по борьбе с киберпреступностью. Несмотря на прогресс, достигнутый в активизации международного сотрудничества в борьбе с киберпреступностью, остаются огромные проблемы.

Несмотря на относительно продолжающийся рост темпов киберпреступности во всем мире, правоохранительные органы изо всех сил пытаются не отставать, что привело к значительному глобальному разрыву в борьбе с киберпреступностью, который позволяет киберпреступникам действовать почти безнаказанно.

Исследование киберпреступности Управления Организации Объединенных Наций по наркотикам и преступности (UNODC) глобальных правоохранительных органов показало, что подавляющее большинство сотрудников правоохранительных органов, опрошенных из 69 государств-членов ООН, заявили, что киберпреступность растет или сильно увеличивается [4].

Рост глобального доступа в Интернет и подключенных к Интернету устройств продолжает предоставлять киберпреступникам все большее число векторов атак для совершения своих преступлений. В 2008 году по всему миру было 1,5 миллиарда интернет-пользователей. В 2018 году Международный союз электросвязи (МСЭ) оценил это число в 3,9 миллиарда – более половины населения мира [5]. Огромное расширение числа интернет-пользователей и сетевых устройств предоставило киберпреступникам бесконечное количество возможностей для их преступлений.

Несмотря на различия в профилях и мотивациях преступников, большинство киберпреступлений были признаны транснациональными по своему характеру. Трансграничный характер Интернета означает, что преступники могут легко создавать совершенно новые категории преступлений, которые могут пересекать границы с помощью нажатий на клавиатуре. Один инцидент с киберпреступностью может поразить бесчисленное множество жертв во многих разных странах независимо от местонахождения преступников, что означает, что расследования киберпреступности должны часто вовлекать правоохранительные органы, прокуроров и судей в нескольких юрисдикциях, государствах. Это создает осложнения для расследований, связанных с киберпреступностью, включая вопросы об экстерриториальной юрисдикции и эффективности механизмов международного сотрудничества.

Комплексное исследование по борьбе с киберпреступностью [6] УНП ООН 2013 года показало, что большинство из почти 70 опрошенных государств-членов ООН не смогли предоставить статистические данные о киберпреступности. Только шесть стран, в основном в Европе, смогли рассчитать среднее количество подозреваемых на количество зарегистрированных преступлений, связанных с незаконным доступом и компьютерным мошенничеством и подделкой документов, что составляет примерно 25 зарегистрированных подозреваемых на 100 преступлений.

Препятствия в достижении прогресса в борьбе с глобальными проблемами в правоохранительных органах многогранны и были хорошо задокументированы в количественных и качественных исследованиях. Их можно разделить на всеобъемлющие категории: технические, операционные, а также стратегические и политические проблемы.

На стратегическом уровне необходимо политическое решение о приоритетности борьбы с киберпреступностью и обеспечения того, чтобы достаточные людские и финансовые ресурсы были выделены для борьбы с угрозой. Однако это может быть серьезной проблемой. В докладе «О практической реализации и функционировании европейской политики по предупреждению киберпреступности и борьбе с ней» Генеральный секретариат Совета Европейского союза (ЕС) установил, что государства-члены ЕС оценили необходимость «высокого уровня политической воли, бюджетных усилий и крупных инвестиций в человеческие и технические ресурсы». Оценка показала, что степень приверженности и эффективности государств-членов ЕС борьбе с киберпреступностью варьировалась [7].

Правительствам также трудно отдавать приоритет киберпреступности над различными формами преступлений, особенно теми, которые, как считается, могут привести к большей гибели людей и более дестабилизирующему воздействию на их страны. Это может быть особенно верно в случаях терроризма. Например, в Великобритании бюджет в размере 1,3 миллиарда фунтов стерлингов, направленный на борьбу с киберпреступностью в течение пяти лет можно сравнить с бюджетом по борьбе с терроризмом в размере более 2 миллиардов фунтов стерлингов в год за тот же бюджетный период. Трудно провести прямое сравнение между такими бюджетами, но это свидетельствует об относительных приоритетах одного правительства со сравнительно широкими возможностями как в области кибербезопасности, так и борьбы с терроризмом. При этом часть финансирования кибербезопасности страны было перенаправлено на борьбу с терроризмом. В докладе о прогрессе Великобритании в реализации Национальной программы кибербезопасности на 2016-2021 годы оценка показала, что более 1/3 выделенного финансирования Программы было переведено на борьбу с терроризмом и другие приоритеты национальной безопасности, задерживая работу над критически важными проектами в сфере кибербезопасности. Следует отметить, что частный сектор также вносит свой вклад в финансирование программ в сфере кибербезопасности, в отличие от мер, направленных на борьбу с терроризмом [8].

На стратегическом уровне также существуют проблемы в установлении четкого разделения компетенции различных государственных учреждений, работающих над вопросами, связанными с кибербезопасностью, и процесса межведомственного взаимодействия. Это часто усугубляется, когда нет центрального органа по надзору в конкретной области. В Соединенных Штатах существует множество государственных учреждений и правоохранительных органов,

участвующих в борьбе с киберпреступностью, которые часто имеют одинаковую компетенцию без главного над ними органа. Это привело к неэффективности, увольнениям и трудностям в обеспечении кибербезопасности США [9].

При этом во многих государствах сформированы стратегии в сфере кибербезопаснсоти, однако, многие из них не всегда связаны с правовой основой и не являются официальными и имеющими реальную юридическую силу, а выступают в качестве декларативных документов.

Тем не менее был замечен некоторый прогресс в этом направлении работы. Например, правительство Сингапура запустило Стратегию кибербезопасности в 2016 году с соответствующим Национальным планом действий по борьбе с киберпреступностью, в котором изложены различные и конкретные действия, которые отдельные учреждения и органы предпринимают для достижения целей стратегии. Также в Сингапуре была учреждена должность министра кибербезопасности, который координирует процесс реализации Стратегии [10].

Эти стратегические трудности в противодействии проблем в борьбе с киберпреступностью связаны с препятствиями в развитии международного сотрудничества в области кибербезопасности и повышении возможностей и технического опыта систем уголовного правосудия различных государств. Хотя за последние пять лет был достигнут прогресс в развитии международного сотрудничества и определении правил и норм поведения государств в киберпространстве, при этом многие государства отказываются от обмена опытом и поддержки друг друга, хоть киберпреступность и имеет трансграничный характер.

Заключение

Киберпреступность привела к созданию новых и развитию существующих видов преступлений, которые могут затронуть несколько государств одним нажатием клавиши.

Трудно оценить точный масштаб глобального вреда от киберпреступности из-за отсутствия показателей киберпреступности и статистики правоприменения, но некоторые исследования показывают, что очень немногие страны добиваются большого прогресса.

Чтобы сократить риски киберпреступности, существует ряд технических, оперативных и политических проблем, которые должны быть решены рядом субъектов государственного и частного секторов, чтобы помочь устранить проблемы в кибербезопасности и повысить уровень борьбы с киберпреступлениями.

Хоть большинство стран признают важность борьбы с киберпреступностью, однако, принимаемые усилия могут быть перераспределены на борьбу с другими важными и опасными явлениями – например, на борьбу с терроризмом.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы на английском языке / References in English

1. Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain // Europol. — URL: https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain (accessed 13.09.2023)

2. Malby S. Comprehensive Study on Cybercrime / S. Malby, R. Mace, A. Holterhof et al. — URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 13.09.2023)

3. Wray A.C. Threats to The Homeland / A.C. Wray. — 2022. — URL: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Wray-2022-11-17.pdf (accessed 13.09.2023)

4. TU Key ICT indicators for developed and developing countries and the world (totals and penetration rates). — URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (accessed 13.09.2023)

5. Report Of The Attorney General's Cyber Digital Task Force. — URL: https://www.justice.gov/archives/ag/page/file/1076696/download (accessed 13.09.2023)

6. The Socio-Economic Impact of Broadband in sub-Saharan Africa: The Satellite Advantage / Commonwealth Telecommunications Organisation. — 2012.

7. Bridge M. Hackers Go Free from Prosecution / M. Bridge // The Times. — URL: https://www.thetimes.co.uk/article/hackers-go-free-from-prosecution-drtld6ncp (accessed 13.09.2023)

8. Miller C. British Police Are on the Brink of a Totally Avoidable Cybercrime Crisis / C. Miller // Wired. — URL: https://www.wired.co.uk/article/british-police-cybercrime-hacking (accessed 13.09.2023)

9. Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime". — URL: https://perma.cc/BNH5-U5AB (accessed 13.09.2023)

10. Ben-Hassineet W. When "Cyber crime" Laws Gag Free Expression: Stopping the Dangerous Trend Across / W. Ben-Hassineet et al. // Mena.