

КИБЕРПРЕСТУПНОСТЬ И ПРАВА ЧЕЛОВЕКА: ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ИХ ВЗАИМОДЕЙСТВИЕ



Тураббаев Хусанбек Абдусаламович
кандидат юридических наук, профессор

Аннотация. В статье раскрыта роль Интернета при совершении преступной деятельности, отмечены существующие пробелы в законодательстве, которые негативно влияют на борьбу с киберпреступлениями и защиту прав человека. Проведен криминалистический анализ вопросов, возникающих при преследовании киберпреступников.

Ключевые слова: права человека, киберпреступность, Интернет, расследование, законодательство, международное право.

KIBERJINOYAT VA INSON HUQUQLARI:

HUQUQIY TARTIBOTNING XUSUSIYATLARI VA ULARNING O'ZARO ALOQADORLIGI

Annotatsiya. Ushbu maqolada Internetning jinoiy faoliyatdagi roli ko'rib chiqilgan, qonunchilikdagi bo'shliqlar, ularning kiberjinoiyatchilikka qarshi kurashishda inson huquqlari ahamiyati ochib berilgan. Shuningdek, kiberjinoiyatchilarni jinoiy javobgarlikka tortishda yuzaga keladigan ayrim masalalarning kriminalistik tahlili berilgan.

Kalit so'zlar: inson huquqlari, kiberjinoiyat, Internet, tergov, qonunchilik, xalqaro huquq.

CYBERCRIME AND HUMAN RIGHTS:

FEATURES OF LEGAL REGULATION AND THEIR INTERACTION

Abstract. This article addresses the role of the Internet in the commission of criminal activity. The article reveals gaps in legislation, and their failure to deal with cybercrime and human rights. On this basis, this article provides a forensic analysis of the issues that arise in the prosecution of cyber criminals.

Keywords: human rights, cybercrime, Internet, investigation, legislation, international law.

В последние годы распространение Интернета было беспрецедентным. Интернет используется как инструмент для развлечения, образования, сервиса, социальных целей, а также для других целей. Благодаря Интернету люди стали ближе друг к другу виртуально. Это создало взаимосвязь и взаимозависимость в глобальной экономике. Многие действия можно совершать не выходя из дома. Несмотря на эти положительные моменты, Интернет создал еще одну среду для преступлений. Киберпреступность представляет опасность не только

для Интернет-предприятий, но и для частных лиц и даже правительств. Например, исследование IBM, проведенное в США, показало, что средняя стоимость утечки данных в 2024 году составила около 4,88 миллионов долларов за инцидент [1]. Именно на этом фоне данное исследование дает представление о киберпреступлениях и правах человека.

Рассмотрим отдельные факторы, препятствующие эффективному раскрытию и расследованию преступлений, совершаемых в Интернет-пространстве. Следует отметить, что доказательства при расследовании кибер-

преступлений, как утверждается, хрупки и легко поддаются порче. Это объясняется тем, что некоторые изоцированные киберпреступники строят свою деятельность таким образом, что при любой попытке получить доказательства жесткие диски самоуничтожаются. В дополнение к этому, трудно обеспечить сохранность доказательств. Для создания дополнительного контекста далее будут рассмотрены конституционные, процессуальные нарушения и нарушения прав человека в контексте расследования киберпреступлений. Это дает возможность изучить процедурные нарушения, допускаемые сотрудниками следственных органов в отношении конституционно закрепленных прав обвиняемого. По сути, поставленные вопросы заключаются в том – соблюден ли надлежащий процессуальный порядок, и в какой степени были нарушены права человека.

Общеизвестно, что существует необходимость согласования государственной практики с конституционализмом, правами человека и соответствующими надлежащими процессами. Здесь изложены некоторые меры, принятые рядом стран для решения проблем, связанных с киберпреступностью, сделана попытка выработать рекомендации, призывающие к реформам.

Как и в большинстве публикаций, посвященных киберпреступности, работу начнем с определения. Следует отметить, что стандартного определения “киберпреступности” не существует. Однако, согласно известным определениям, киберпреступность включает в себя любую преступную деятельность, которая осуществляется через компьютеры или сети. Интересно отметить, что во многих случаях киберпреступлений меньше, а традиционных элементов больше. По словам британского ученого Давида С. Уолла, многие правонарушения уже существуют в обычной системе уголовного правосудия. В качестве примера можно привести такие правонарушения, как педофилия, мошенничество и порнография [3]. Соответственно, существует

дискуссия о том, следует ли разрабатывать категории киберпреступлений или эти преступления следует понимать через призму существующих преступлений. Таким образом, очевидно, что при концептуализации киберпреступлений будет оставаться проблемой, происходят ли эти преступления в виртуальном или реальном мире. Это взаимодействие между виртуальным и реальным миром продолжает вносить путаницу в классификацию киберпреступлений. Д. Уолл классифицирует эти преступления на 3 группы:

1. Преступления против целостности компьютера (преступления против машинных систем);
2. Преступления с использованием компьютера (преступления с использованием машинных систем);
3. Преступления компьютерного содержания (киберпорнография, кибернасилие).

В контексте киберпреступлений эти категории должны быть достаточно широкими, чтобы охватить любой вид киберпреступлений. Помимо этого общего понятия, существует также множество различных форм киберпреступлений. В замечательной статье под названием “Трансформационные аспекты киберпреступлений” индийский ученый М.Н. Сирохи описывает эти формы как разновидности киберпреступлений [4]. Затем он объясняет основные их разновидности: киберсталкинг, хакерство, фишинг, межсайтовый скриптинг, вишинг и киберсквоттинг. Основным преступлением в контексте киберпреступности является хакерство, которое подразумевает нацеливание на сам компьютер [5]. Обычно это включает в себя взлом компьютера или компьютерной системы, преднамеренное повреждение или нанесение ущерба и несанкционированный перехват компьютерных данных.

При анализе киберпреступлений интересно отметить, что в Интернете трудно установить вопрос о географических границах и серверах. Тем не менее, были приняты законы, направленные на регулирование

киберпреступлений. Хотя международной конвенции не существует, хороший законодательный акт можно найти в контексте Европейского Союза. Совет Европы принял Конвенцию о киберпреступности (2001 г.). Она известна как Будапештская конвенция [2].

Стоит отметить, что Будапештская конвенция, однако, также открыта для принятия другими сторонами. Основная цель конвенции – дать ответ на вызовы, возникающие в связи с развитием цифровой платформы. Будапештская конвенция считается наиболее значимым международным соглашением по киберпреступности и электронным доказательствам. В преамбуле Будапештской конвенции говорится о международном сотрудничестве в борьбе с киберпреступлениями [6].

Это связано с тем, что в некоторых случаях преступники могут проживать не в той стране, в которой они фактически совершили преступление. Одной из проблем, актуальных при расследовании киберпреступлений, является проблема экстрадиции, когда сотрудничество может быть затруднено. Поэтому вполне логично, что Будапештская конвенция считает необходимым международное сотрудничество. В основе Будапештской конвенции лежит понимание необходимости предотвращения неправомерного использования сетей, систем и данных путем установления уголовной ответственности за определенные действия или поведение. Конвенция также осознает необходимость соблюдения основных прав человека, закрепленных в Конвенции Совета Европы о защите прав человека и основных свобод [7], Международном пакте ООН о гражданских и политических правах 1966 года [8] и других применимых международных договорах по правам человека. Что касается надлежащих процедур, то Конвенция содержит конкретные требования к членам, присоединившимся к ней. Так, согласно ст. 14, государства-члены обязаны принять законодательные и иные меры, необходимые для проведения уголовных расследований или разбирательств. С точки зрения прав чело-

века, Конвенция также создает обязательство в соответствии со статьей 15 должным образом учитывать права человека при установлении, осуществлении и применении полномочий и процедур. Далее Конвенция предоставляет свободу действий для принятия законодательства в отношении поиска и изъятия хранящихся компьютерных данных и получения данных о содержимом в соответствии со статьями 19 и 21, соответственно.

Появление киберпреступности как одного из самых серьезных преступлений в мире поставило перед правоохранительными органами новые задачи.

Одна из самых больших проблем, стоящих перед правоохранительными органами, связана с созданием законов против киберпреступности, поскольку в некоторых юрисдикциях не существует нормативно-правовых актов, охватывающих данный вопрос. Это связано с тем, что в некоторых юрисдикциях киберпреступность все еще считается новым явлением, особенно в странах третьего мира, где многие люди становятся жертвами киберпреступников. Согласно исследованию австралийского профессора Сюзан В. Бреннер, было установлено, что более 100 стран не имеют уголовного законодательства, достаточного для борьбы с киберпреступностью. Другое её исследование, в котором изучалось уголовное законодательство пятидесяти двух стран, показало, что тридцать три из них еще не обновили свои законы для борьбы с любым видом киберпреступности. Это свидетельствует о том, что в плане законодательства или международных статутах для обуздания этих киберпреступников практически ничего не сделано [9].

По причине отсутствия законов о привлечении киберпреступников к ответственности число кибератак продолжает расти ежегодно, в то время как количество судебных процессов по киберпреступлениям, как уголовных, так и гражданских, снижается. В некоторых юрисдикциях существует множество законов о киберпреступлениях, но их исполнение – это

уже другой вопрос. Жертвы таких преступлений чувствуют несправедливость, когда преступники не привлекаются к ответственности. Это происходит по ряду причин, которые мешают сотрудникам правоохранительных органов выполнять свои обязанности, поскольку киберпреступления отличаются от обычных преступлений, с которыми они всегда имели дело. Одна из основных причин, по которой в Соединенных Штатах мало успешных судебных дел, заключается в требованиях, которые необходимы для того, чтобы благополучно подать иск о нарушении данных. Для успешного судебного разбирательства жертвам утечки данных необходимо доказать “ущерб на самом деле” или то, что понесенный ими ущерб был конкретным и определенным, фактическим или неизбежным, а не предположительным или гипотетическим. Это часто трудно доказать, поскольку ущерб должен был возникнуть в результате утечки личной информации. Руководитель американских спецслужб по борьбе с киберпреступлениями Мелисса МакДонаф также утверждает, что жертвы киберпреступлений не могут доказать халатность со стороны компании, владеющей их персональной информацией, которая была бы взломана киберпреступниками. Далее МакДонаф отмечает, что это требование закона США о доказательстве “фактического ущерба” не позволяет многим делам даже возникнуть [10].

При передаче дела о киберпреступлении в суд, правоохранительные органы сталкиваются с различными проблемами. Первая проблема – атрибуция: обычно очень трудно найти реального человека, ответственного за киберпреступление. Это связано с тем, что киберпреступники обычно маскируют место своего происхождения, используя различные инструменты и методы сокрытия, такие как виртуальные частные сети.

Второй проблемой, которая является самым большим препятствием для передачи киберпреступлений в суд – тот факт, что киберпреступления являются цифровыми и

обычно пересекают границы стран. Многие хакеры действуют на международном уровне, что не позволяет сотрудникам правоохранительных органов преследовать этих лиц без экстрадиции. Например, в Узбекистане многие киберпреступления, направленные против граждан и компаний, обычно совершаются из других стран, как например, Китай, Россия и США. Это определенным образом влияет на то, как сотрудники правоохранительных органов и подразделения МВД Республики Узбекистан по борьбе с киберпреступлениями осуществляют свою деятельность, поскольку они не имеют юрисдикции в этих странах, а в некоторых случаях, между этими странами нет договоров об экстрадиции. Это подтверждает тот факт, что такие страны, как Япония, являются убежищем для киберпреступников, поскольку у них нет договора об экстрадиции с Узбекистаном, что, несомненно, усложняет процесс их поимки.

Другим фактором, который также затрудняет вынесение обвинительных приговоров, является вопрос о характере доказательств, доступных для киберпреступлений. Проблема с цифровыми доказательствами заключается в том, что они отличаются от обычных доказательств, поскольку являются хрупкими и могут быть легко потеряны или испорчены. Поэтому обеспечение целостности доказательств и поддержание четкой цепочки хранения цифровых доказательств является сложной задачей. Этому не способствует тот факт, что некоторые изоэренные киберпреступники могут настроить свои компьютеры на автоматическое уничтожение доказательств при доступе к ним кого-либо, кроме них самих. Проблемы, связанные с расследованием киберпреступлений, если их не решать тщательно, могут привести к будущим спорам между правительствами, о чем свидетельствуют недавние заявления для прессы Великобритании и США. Эти две страны обвиняют российское правительство в проведении скоординированной кампании по атаке и компрометации государственных сетей, частных

компаний и поставщиков услуг критической инфраструктуры [11].

Интересная перспектива для размышления: какие нарушения происходят в контексте борьбы с киберпреступлениями. В попытке выследить преступников многие государства нарушают основные права в области Интернета. Например, имели место попытки и реальные нарушения права на неприкосновенность частной жизни. Чтобы проиллюстрировать этот факт, можно рассмотреть неспособность государств получить постановление на проведение обыска при расследовании киберпреступлений. В США правительство попыталось принять Закон о борьбе с пиратством в Интернете, который предусматривал массовую слежку. Однако этот закон был отвергнут миллионами американцев на том основании, что во имя борьбы с пиратством будет введена цензура в Интернете. Еще одна проблема, получившая распространение в Соединенных Штатах Америки, – это подстрекательство. В данном случае правительство подстрекает людей, предрасположенных к совершению определенного правонарушения, к его совершению. Хорошим примером является ситуация, когда государство побуждает хакера взломать определенный компьютер в обмен на деньги, а затем арестовывает конкретного человека. Это, по мнению ряда ученых, представляет собой конституционный вопрос. То есть, если бы не вмешательство государства, преступление не было бы совершено. В Пекине предприятия, предоставляющие Интернет-услуги, были обязаны установить государственное шпионское программное обеспечение, иначе их лицензии будут аннулированы. Это подкрепляет аргумент о том, что правительства не обязательно заботятся о правах, пытаясь задержать преступления в Интернете. Помимо этих существенных вопросов, проблемы, связанные с преследованием киберпреступлений, затрагивают и процедурные вопросы. Правам лиц, совершивших киберпреступления, не уделяется должного

внимания. Например, осужденным за киберпреступления в Китае было отказано в соблюдении процессуальных норм. Кроме того, многие приговоры не соответствуют совершенным преступлениям. Например, Цао Хайбо был приговорен к 8 годам лишения свободы за продвижение демократии в Интернете [12]. Это дает основание утверждать, что необходимы четкие процедуры расследования киберпреступлений, судебного разбирательства и вынесения приговоров.

Интернет как платформа по-прежнему предоставляет множество возможностей. Вместе с тем, Интернет создает ряд проблем в сфере управления. Самый главный из них – как странам следует поступать с правонарушителями в Интернете? Как уже говорилось, проблема начинается с отсутствия консенсуса относительно того, что является киберпреступлением и какие права должны быть предоставлены в Интернете. Эта неопределенность дает возможность странам нарушать процедуры, а также права пострадавших. Именно на этом фоне предлагается разработать международную конвенцию, которая будет подписана и принята всеми странами. На самом деле в международном праве существует вакуум в этом отношении. Хотя Будапештская конвенция Европейского Союза хорошо формулирует ряд киберпроблем, этот документ не имеет веса международного документа из-за присущего ему регионального характера. Создание такой конвенции, среди прочего, способствовало бы пониманию киберпреступлений. Более того, единый подход к киберпреступлениям особенно полезен в том смысле, что в Интернете существует множество вопросов юрисдикции. Во многих случаях правонарушение носит трансграничный характер, поэтому введение различных стандартов разными странами затруднит анализ. Еще одно предложение заключается в том, что все государства должны взять на себя обязательство соблюдать права человека в Интернете. Тот факт, что определенные операции происходят виртуально, не отменяет

того факта, что права человека неизменно должны соблюдаться. Соответственно этому, должна быть разработана теория Интернет-прав человека. Государства должны опираться на работу, которая была проделана над необязательной резолюцией Совета по правам человека ООН по поощрению, защите и осуществлению прав человека в Интернете. В эту работу также следует включить содержание Будапештских конвенций в части, касающейся киберпреступлений и прав человека. Важно отметить, что государства должны четко определить процедуры, которым необходимо следовать при преследовании киберпреступников. Такая ясность устранил

произвол и заставит государства следовать надлежащему процессу при рассмотрении киберпреступлений. Нынешняя туманность в отношении процедуры, которой необходимо следовать, стимулирует государства использовать возможность пренебречь надлежащей правовой процедурой. С этим тесно связана и ясность в вопросе о том, какое наказание следует назначать за киберпреступления. Однако следует помнить, что при наличии предикатных преступлений они также должны приниматься во внимание при вынесении приговора.

Использованные источники

1. Отчет о стоимости утечки данных в 2021 году. – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.ibm.com/security/data-breach> (Дата обращения 15.02.2022).
2. Конвенция Совета Европы о киберпреступности (Будапештская конвенция). – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Дата обращения 15.02.2022).
3. David S. Wall. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge, UK: Polity Press, 2007. ISBN 9780745627366 – 288 p.
4. M.N. Sirohi. Transformational Dimensions of Cybercrime. – ND, India: Alpha Editions, 2015. ISBN 10: 8193142233 ISBN 13: 9788193142233 – 290 p.
5. Энциклопедия «Касперского» / База знаний / Уязвимости и хакеры / Кто такие «хакеры». – [Электронный ресурс] – Доступен по ссылке. – URL: <https://encyclopedia.kaspersky.ru/knowledge/who-is-hacker/> (Дата обращения 17.02.2022).
6. Н.И. Долженко, И.Г. Хмелевская. К вопросу о содержательных аспектах киберпреступности. – Научная статья NOMOTHETIKA: Философия, Социология, Право. 2020. Том 45, № 2, С 315–322.
7. Конвенции Совета Европы о защите прав человека и основных свобод. – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols> (Дата обращения 17.02.2022).
8. Международном пакте ООН о гражданских и политических правах 1966 года. – [Электронный ресурс] – Доступен по ссылке. – URL: [https://www.legislationline.org/ru/documents/id/14580#:~:text=\(Дата обращения 17.02.2022\).](https://www.legislationline.org/ru/documents/id/14580#:~:text=(Дата обращения 17.02.2022).)
9. Susan W. Brenner. Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law. Volume 8, Number 2 (June 2001). – [Электронный ресурс] – Доступен по ссылке. – URL: <http://classic.austlii.edu.au/au/journals/MurUEJL/2001/8.html> (Дата обращения 18.02.2022).
10. Melissa McDonough. The Difficulties of Litigating Cyber Crime. / Chiefs, Cyber Crime Investigations, Emerging Threats, Legal, Prosecutors. March 30, 2016. – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.iacpcybercenter.org/the-difficulties-of-litigating-cyber-crime/> (Дата обращения 18.02.2022).
11. Warwick Ashford. UK and US accuse Russia of targeting network infrastructure. 16 Apr 2018 19:00. – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.computerweekly.com/news/252439099/UK-and-US-accuse-Russia-of-targeting-critical-infrastructure> (Дата обращения 19.02.2022).
12. Official website of the Promoting human rights & empowering grassroots activism in China. (April 3, 2013) – [Электронный ресурс] – Доступен по ссылке. – URL: <https://www.nchrd.org/2013/04/submission-to-un-on-caohai-bo-april-1-2013/> (Дата обращения 19.02.2022).