УДК 34 **DOI: 10.34670/AR.2023.15.36.035**

Международное уголовно-правовое противодействие преступлениям в сфере информационной безопасности

Лихачев Никита Александрович

Аспирант кафедры уголовного права и криминологии
Кубанский государственный университет,
350075, Российская Федерация, Краснодар, ул. Ставропольская, 149;
e-mail: Nik.likhachev.97@bk.ru

Аннотация

Данная статья посвящена проблемам международного уголовно-правового противодействия преступлениям в сфере информационной безопасности, показатели преступности, степень цифровизации общества. Автором анализируются различные международные соглашения (Окинавская хартия глобального информационного общества, Конвенция о преступности в сфере компьютерной информации, Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности) их достоинства и недостатки. Анализируются перспективы уголовно-правового определения дефиниции «информационная война», которая уже закреплена на международном уровне, возможность имплементации данных норм в отечественное уголовное законодательство. В заключении приводятся выводы и предложения, направленные на совершенствование уголовно-правового противодействия преступлениям в сфере информационной безопасности.

Для цитирования в научных исследованиях

Лихачев Н.А. Международное уголовно-правовое противодействие преступлениям в сфере информационной безопасности // Вопросы российского и международного права. 2023. Том 13. № 4А. С. 438-443. DOI: 10.34670/AR.2023.15.36.035

Ключевые слова

Информационная безопасность, информационная война, уголовно-правовое противодействие, международное право.

Введение

Преступления против информационной безопасности являются проблемой транснационального и международного уровня. Актуальный уровень развития компьютерных технологий, способов и средств распространения и передачи информации в любых формах позволяет совершить преступление в любом месте из любой точки планеты.

По различным оценкам, в 2022 году ежесекундный поток Интернет-трафика в мире составил 150 700 гигабайт [Global Business Data Platform Statista, www…]. Тенденция к росту в перспективе не только сохранится, но и будет увеличиваться пропорционально росту населения и увеличения цифровизации в развивающихся странах. Согласно статистике, Social 2020 среднестатистический человек в среднем проводит в интернете 6 часов ежедневно [Вся статистика интернета на 2020 г., www…]. Рост цифрового потенциала является определяющим в будущем развитии государств, их роли на международно-политической арене, степени их влияния, уровне жизни и довольства населения.

Основная часть

К наиболее актуальным преступлениям в сфере информационной безопасности на международном уровне относят киберпреступления, информационный терроризм и экстремизм, распространение заведомо ложных сведений, преступления против собственности, совершаемые с применением информационно-телекоммуникационных технологий.

Первые шаги в формировании международных норм, направленных на обеспечение информационной безопасности, были предприняты при создании Организации Объединенных наций и последующем принятия Всеобщей декларации прав человека. Ст. 19 Декларации гарантирует право на свободу убеждений, а также свободу поиска, получения и распространения информации любыми идеями вне зависимости от государственных границ. Ст. 12 гарантирует неприкосновенность личной и семейной жизни, тайны корреспонденции, а также честь и репутации. В результате произойдет постепенное формирование системы обеспечения международной информационной безопасности.

На уровне главной международной общественной организации – ООН тема информационной безопасности возникла в 1998 г., когда по предложению Российской Федерации была принята первая резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998 г., www…], что положило начало обсуждения проблем международной информационной безопасности в ООН.

Впоследствии были принята Окинавская хартия глобального информационного общества от 22 июля 2000 г. [Окинавская хартия глобального информационного общества от 21 июля 2000 года, www…] Значение этого документа заключается в том, что информационные-телекоммуникационные технологии признаются ключевым фактором, определяющим развитие XXI века. П. 5 Хартии призывает суверенные государства к развитию информационных технологий, формировать партнерство между всеми участниками в этой сфере.

Современная международная архитектура по противодействию преступлениям в сфере информационно-телекоммуникационных технологий во многом базируется на Конвенции Совета Европы о киберпреступности, принятой в Будапеште в 2001 г. В результате принятия к данной конвенции Протокола №1 была дана официально правовая классификация преступлениям в сфере киберпресутпности [Конвенция о преступности в сфере компьютерной

информации ETS N 185 (Будапешт, 23 ноября 2001 г.)., www…]:

1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

– противозаконный доступ;

– противозаконный перехват;

– воздействие на данные;

– воздействие на функционирование системы;

– противозаконное использование устройств;

2) правонарушения, связанные с использованием компьютерных средств:

– подлог с использованием компьютерных технологий;

– мошенничество с использованием компьютерных технологий;

3) правонарушения, связанные с содержанием данных:

– преступления, связанные с детской порнографией;

4) правонарушения, связанные с нарушением авторского права и смежных прав.

Российская Федерация так и не подписала данную конвенцию, хотя количество стран-подписантов ежегодно растет (более 50 государств-подписантов). Позиция Российской Федерации заключается в принципиальном непринятии ст. 32 п. b, доскональное исполнение которого влечет нарушение внутреннего информационного суверенитета государства, так как он предусматривает возможность «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их».

Полагаю, что перспективным является продолжение развития и совершенствования Соглашения о сотрудничестве в области обеспечения международной информационной безопасности в рамках Шанхайской организации сотрудничества от 16.06.2009 г.

Итогом принятия Соглашения стало официальное международно-правовое закрепление «основных понятий в области обеспечения международной информационной безопасности», среди которых особо выделяются «информационная война», «информационное оружие», «информационная преступность», «информационный терроризм», «информационное пространство» и т.д.

В приложении 2, принятом в качестве дополнения к Соглашению, излагается подробный перечень информационных преступлений, таких как:

– незаконное проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации;

– умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ;

– осуществление DDoS-атак (отказ в обслуживании) и иных негативных воздействий;

– причинение ущерба информационным ресурсам;

– нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни;

– использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т. д.

В 2021 г. Российская Федерация внесла еще один проект Конвенции «О противодействии использованию информационно-коммуникационных технологий в преступных целях», содержащий ряд важных определений, таких как вредоносная компьютерная программа, информация, информационно-телекоммуникационные сети, компьютерная атака, объекты критической инфраструктуры и т.д. Предлагает универсальную криминализацию целого ряда

преступлений, в том числе таких, которые не содержатся в отечественной редакции УК РФ, а именно:

– нарушение функционирования информационно-коммуникационных сетей;
– неправомерное воздействие на цифровую информацию;
– неправомерный перехват;
– создание и использование цифровой информации для введения пользователя в заблуждение (умышленного противоправного создания и использования цифровой информации, сходной до степени смешения с уже известной пользователю и вызывающей доверие информацией, повлекшее причинение существенного ущерба).

Решение данной проблемы могло бы заключаться в принятии такой Всеобъемлющей Конвенции на уровне ООН, а также создание на ее базе впоследствии международной организации с справедливым и равным представительством государств-подписантов. Задачей бы этой организации являлось формирование единой универсальной системы доменных имен (IP-адресов) и последующего контроля над ней. Это позволило бы при расследовании преступлений определять юрисдикцию и в двухстороннем порядке обмениваться данными о предполагаемом преступнике.

Массовый характер совершения преступлений против информационной безопасности лишний раз свидетельствует о необходимости универсализации международно-правовой нормативной базы, а после этого и национального уголовного законодательства, обменом опыта расследования подобных преступлений и совместной координации противодействия.

Отметим, что определение информационной войны, официально принятое ШОС предусматривает ряд составов преступлений, предусмотренных УК РФ, что позволяет относить данный термин к уголовно-правовой науке. Однако в настоящий момент дефиниция «информационная война», представленная в политологии, философии, филологии и ряде гуманитарных наук, не имеет своего содержания в уголовно-правовой науке.

Несмотря на наличие уже принятых международно-правовых актов в сфере обеспечения информационной безопасности, их практическая значимость относительно не велика. На сегодняшний день в мире нет универсального определения понятия преступлений против информационной безопасности, нет четкого перечня составов преступлений и их классификации. Да, следует отметить положительную роль Будапештского и Шанхайского акта, однако они являются актами континентального, но никак не всеобъемлющего уровня. К тому же они обладают силой акта «мягкого права» и выражают в большей степени лишь политическую волю и позиции государств-подписантов. Международному сообществу только лишь предстоит создать единую систему обеспечения информационной безопасности. В большей степени успешность подобных действий зависит от политической воли, желания и договоренности Великих держав, возможности нахождения между ними приемлемого консенсуса.

Заключение

Подводя итог, необходимо отметить, что единственным способом эффективного уголовно-правового противодействия преступлениям в сфере информационной безопасности является принятие всеобъемлющей конвенции, которая определит понятийно-категориальный аппарат, перечень преступлений и их состав, понятие и критерии информационной войны, порядок координации и взаимодействия правоохранительных органов. При этом условие соблюдение цифрового и информационного суверенитета государств должно быть ключевым при выработке

итогового документа.

Понятие информационной войны должно закрепиться в теории уголовного права, так как на международном уровне оно уже получило свое официальное и нормативное определение. Необходимо рассматривать информационную безопасность не только в контексте преступлений в сфере компьютерной информации, но и тех уголовно-правовых деликтов, которые связаны с распространением информации различного свойства и содержания, как способа совершения противоправного деяния. Необходима теоретическая разработка уголовно-правового противодействия информационным войнам, определения критериев противоправности, степени общественной опасности и общественно опасных последствий.

Библиография

1. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях Проект 29.06.2021 URL:https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf. (Дата обращения 20.04.2023 г.).
2. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#s6sltZT8ojzV24w91.
3. Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Вместе с <Перечнями основных понятий и видов угроз, их источников и признаков>) (Заключено в г. Екатеринбурге 16.06.2009) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#Kf6mtZTeqMcadQ9Z1. (Дата обращения 20.03.2023 г.).
4. Global Business Data Platform Statista //URL: https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/ (Дата обращения 20.04.2023 г.).
5. Вся статистика интернета на 2020 г. – цифры и тренды в мире и в России // Web Canape, 03.02.2020 URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (Дата обращения 20.04.2023 г.).
6. Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998 г. // URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement. (Дата обращения 20.04.2023 г.).
7. Окинавская хартия глобального информационного общества от 21 июля 2000 года. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=d oc&base=INT&n=8382#AuSltZTJodXDwttG. (Дата обращения 20.04.2023 г.).
8. Канюков Н. А., Яхонтова И. М. Международный опыт развития информационных технологий (Окинавская хартия глобального информационного общества) //Colloquium-journal. – Голопристанський міськрайонний центр зайнятості, 2019. – №. 3-4 (27). – С. 16-19.
9. Фастович Г. Г., Багиров С. И. О. Правовое значение окинавской хартии в информационном праве //Аллея науки. – 2019. – Т. 2. – №. 4. – С. 67-72.
10. Сулимин А. Н. Новые формы управления в глобальной информационной среде и проблемы национальной безопасности РФ //Вопросы управления. – 2015. – №. 4 (16). – С. 56-60.

International criminal legal counteraction to crimes in the sphere of information security

Nikita A. Likhachev

Postgraduate student,
Kuban State University,
350075, 149, Stavropol'skaya str., Krasnodar, Russian Federation;
e-mail: Nik.likhachev.97@bk.ru

Abstract

This article is devoted to the problems of international criminal law counteraction to crimes in the field of information security, crime rates, the degree of digitalization of society. The author analyzes various international agreements (the Okinawa Charter of the Global Information Society, the Convention on Crime in the Sphere of Computer Information, the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security), their advantages and disadvantages. The prospects for the criminal law definition of the definition of "information war", which is already fixed at the international level, the possibility of implementing these norms in the domestic criminal legislation are analyzed. In conclusion, conclusions and proposals are presented aimed at improving the criminal law counteraction to crimes in the field of information security.

For citation

Likhachev N.A. (2023) Mezhdunarodnoe ugolovno-pravovoe protivodeistvie prestupleniyam v sfere informatsionnoi bezopasnosti [International criminal legal counteraction to crimes in the sphere of information security]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (4A), pp. 438-443. DOI: 10.34670/AR.2023.15.36.035

Keywords

Information security, information warfare, criminal law counteraction, international law.

References

1. United Nations Convention on the Prevention of the Criminal Use of Information and Communication Technologies Draft 06/29/2021 URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf.
2. UNGA Resolution A/RES/53/70 of December 4, 1998 // URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf ?OpenElement. (Accessed 20.03.2023).
3. Okinawa Charter for the Global Information Society, July 21, 2000. // ATP "ConsultantPlus". URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=8382#AuSltZTJodXDwttG.
4. Computer Crime Convention ETS N 185 (Budapest, November 23, 2001). // ATP "ConsultantPlus". URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#s6sltZT8ojzV24w91.
5. Agreement between the Governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security (Together with the <List of basic concepts and types of threats, their sources and signs>) (Concluded in Yekaterinburg on June 16, 2009) // ATP "ConsultantPlus ". URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#Kf6mtZTeqMcadQ9Z1. (Accessed 20.03.2023).
6. Global Business Data Platform Statista //URL: https://www.statis-ta.com/statistics/631151/worldwide-data-collected-by-smart-buildings/ (Accessed 03/20/2023).
7. All Internet statistics for 2020 - figures and trends in the world and in Russia // Web Canape, 02/03/2020 URL: https:// www.web-canape.ru/business/internet-2020-globalnaya-statistika-i -trendy/ (Accessed 03/20/2023).
8. Kanyukov N. A., Yakhontova I. M. International experience in the development of information technologies (Okinawa Charter of the Global Information Society) //Colloquium-journal. – Holoprystan Regional Employment Center, 2019. – no. 3-4 (27). - S. 16-19.
9. Fastovich G. G., Bagirov S. I. O. Legal significance of the Okinawan charter in information law // Alley of Science. - 2019. - Vol. 2. - No. 4. - S. 67-72.
10. Sulimin A. N. New forms of management in the global information environment and problems of national security of the Russian Federation // Issues of management. – 2015. – no. 4 (16). - S. 56-60.