УДК 34 **DOI: 10.34670/AR.2024.24.13.004**

Особенности правовой охраны информационно-цифрового пространства современной России в условиях информационной войны

Михаленко Никита Алексеевич

Аспирант,
Самарский государственный экономический университет,
443090, Российская Федерация, Самара, ул. Советской Армии, 141;
e-mail: bote2018@gmail.com

Аннотация

В статье рассматриваются актуальные проблемы мирового сообщества в целом, и в частности России, связанные с таким видом киберпреступности, как кибертерроризм. Кибертерроризм, характеризующийся высоким уровнем латентности, а также масштабностью и последствиями, представляет угрозу для информационно- цифрового пространства не только современной России, но и для других стран. Автор отмечает, что в настоящее время наблюдается целенаправленный и координированный характер кибератак, поэтому их опасность кибератак заключается в том, что кибертеррористы могут атаковать даже системы автоматического управления объектов инфраструктуры. Автором выводятся причины кибертерроризма, а также делается вывод о том, что эффективная борьба с кибертерроризмом требует разработки надлежащей правовой базы, которая бы определила понятие кибертерроризма и его уголовно-правовую характеристику. Данная правовая база должна постоянно и динамично развиваться в связи с быстрым развитием информационно- цифрового технологий, а также должна адаптироваться к новым угрозам. Разработка правовой базы и установление единого определения кибертерроризма являются неотъемлемыми шагами для эффективной борьбы с угрозой кибертерроризма. Постоянное обновление и совершенствование правовой базы, а также укрепление международного сотрудничества помогут справиться с растущей угрозой кибертерроризма и обеспечить безопасность в киберпространстве.

Для цитирования в научных исследованиях

Михаленко Н.А. Особенности правовой охраны информационно-цифрового пространства современной России в условиях информационной войны // Вопросы российского и международного права. 2023. Том 13. № 11А. С. 32-38. DOI: 10.34670/AR. 2024.24.13.004

Ключевые слова

Информационно-цифровые технологии, информационная безопасность, киберпреступность, киберпространство, кибертерроризм, кибератаки, международное сообщество.

Введение

Принципиальное значение для развития государственности и национальной безопасности имеет охрана информационно- цифрового пространства современной России. Государственная безопасность – это состояние защищенности интересов России от внутренних и внешних угроз.

На современном этапе развития цивилизации, человечество вступило в информационную эпоху и становление цифровых технологий, которые стремительным образом вырабатываются и внедряются во все сферы общественной жизни. Происходит новый виток формирования цивилизованного общества. Информационно-цифровая трансформация поэтапно охватывает все сферы жизнедеятельности человека, деятельность общества и государства. Поэтому диапазон цифровизации имеет широкий спектр применения.

Развитие сферы информационно-цифровых технологий и их внедрение в правовое пространство России, в экономику страны, стало одним из приоритетных направлений государственной деятельности, о чем свидетельствует принимаемые стратегические и программные документы.

Становление информационно-цифровых технологий, способствуют не только цивилизованному прогрессу общества, но криминализации преступлений связанных с появлением цифровых технологий. Впрочем, стоит отметить, что научно-технический прогресс всегда являлся сопутствующим элементом не только развития цивилизации, но и появлению новых форм преступных посягательств.

Как отмечается в стратегических документах России, внедрение информационно-цифровых технологий, имея положительные моменты, также несут в себе определенные риски, что приводит к необходимости упрочения защиты.

Выработка мер по развитию нормативно-правового обеспечения информационной безопасности российского государства, вызывает необходимость переосмысления разных аспектов в сфере противодействия и борьбы с киберпреступлениями, а в особенности с кибертерроризмом, а также комплексного подхода для разрешения данной проблемы, поскольку надлежащее установление и обеспечение безопасности, напрямую связано с уровнем развития страны.

Основная часть

Обеспечение информационной безопасности является одной из сложнейших теоретико-прикладных проблем, носящих глобальный и всеобъемлющий характер, которая является в равной степени важной как для любого человека, так и государства, и мирового сообщества в целом [Агабалаев, 2009, 5].

Информация в настоящее время в мире становится стратегическим ресурсом. Сегодня охрана информационно-цифрового пространства России выступает в качестве одного из базовых направлений безопасности страны.

Информационная безопасность является состоянием защищенности информации от угроз. Как представляется, под угрозами безопасности информации следует понимать совокупность условий и факторов, которые создают опасность несанкционированного доступа, включая как случайный доступ к информации, так и иные неправомерные действия.

Киберпреступность является серьезной проблемой не только каждого отдельно взятого государства, но и морового сообщества. Угрозы, которые она несет, могут быть связаны с

нарушением конфиденциальности, а также надежности, целостности и доступности информации. В нарушении неприкосновенности частной жизни, утечке данных, несанкционированном доступе или разглашении, в нарушении надежности информации, фальсификация данных или их подделке. Нарушения могут относиться к искажению, ошибкам в передаче информации, утрате данных и блокировании доступа к информации, отключению коммуникаций, технических средств, что представляет собой нарушение доступности.

Как отмечается в литературе, киберпреступность характеризуется высоким уровнем латентности, а также масштабностью, которая сопряжена с тем, что преступление может быть совершено в любом месте расположения сетевых ресурсов [Буз, 2019, 82].

При этом по последствиям, а также масштабу охвата, наибольшую угрозу представляет кибертерроризм, представляющий угрозу для информационно- цифрового пространства современной России.

На российский бизнес, ежедневно приходится более 170 кибератак [Самые крупные кибератаки 2023 года, www], что может быть сопряжено, в том числе, с подрывом российской экономики. Так, например, 05.07.2023 г. РЖД было сообщено, что ее сайт (приложение) было подвергнуты кибератаке [Сайт и приложение РЖД подверглись массированной хакерской атаке, www].

В 2023 г. было также отмечено 12 случаев (по состоянию на 16.11.2023 г.) утечки информации по программам Сбербанка[1], образовательного портала «GeekBrains», «Ашан» и т.д.[2]

Увеличилось количество DDoS-атак на сервисы банков, в том числе Сбербанка, «Уралсиб», Росбанк, «Ак Барс» банк, Уральский банк реконструкции и развития [Самые крупные кибератаки 2023 года, www].

Кибератаки были целенаправленны и, как правило, носили координированный характер. Опасность таких кибератак заключается в том, что кибертеррористы могут атаковать даже системы автоматического управления объектов инфраструктуры[3]. Такие примеры уже известны мировому сообществу.

Так, например, отмечается, что в октябре 2023 года, была произведена кибератака на электросеть Ирана, что привело к масштабным сбоям в функционировании энергосетей [Израильские хакеры вызвали массовые сбои в электросети Ирана, www].

Причинами кибертерроризма послужили несколько аспектов.

Прежде всего, это развитие сетевых компьютерных структур, основанных на информационно-цифровых технологиях.

Кроме того, это глобализация и рост мировой и национальных экономик, а также насыщенность новыми телекоммуникационными технологиями жизненно важных сфер общества.

К причинам кибертерроризма стоит также отнести высокую степень анонимности, которой обладают кибертеррористы в сетевом пространстве, что ведет к высокой латентности преступлений.

---

[1] «СберСпасибо», онлайн-платформы правовой помощи «СберПраво», «СберЛогистики» (сервис «Shiptor»).

[2] В том числе : «Твой Дом»,»Леруа Мерлен», сайты Gloria Jeans, book24.ru, «Аскона», «Буквоед», «ТВОЕ», «Читай-город», edimdoma.ru, «АСТ» и «Эксмо».

[3] Водоканалов, электростанций и т.п.

Помимо этого, стоит обратить внимание на фактор мобильности кибертеррористов. Интернет находится в трансграничном пространстве, не имеющем визуальных границ, что позволяет кибертеррористам устранить необходимость прохождения контрольно-пропускных пунктов, границ или таможенных проверок. Интернет также устраняет необходимость нахождения вблизи цели, на которую планируется совершение кибератаки.

Более того, при кибертерроризме сокращает потребность в психологической и физической подготовке, которая требуется при традиционных формах терроризма. Таким образом, кибертерроризм отличается от традиционных методов терроризма, поскольку позволяет нанести удар по большому количеству людей, а также вывести системы инфраструктуры из строя.

Эффективная борьба с кибертерроризмом требует разработки надлежащей правовой базы, которая бы определила понятие кибертерроризма и его уголовно-правовую характеристику. В настоящее время стоит сложная задача отделения кибертерроризма от остальной киберпреступности.

Ни российские, ни зарубежные ученые пока не пришли к единому определению кибертерроризма, которое бы позволило четко разграничить акты кибертерроризма от других преступлений в области информационно-цифровой информации [Антонян, Аминов, 2019, 173].

При этом некоторые ученые придерживаются определения Д. Денинга, который определил его через слияние киберпространства и терроризма, где ведутся противозаконные действия, посредством угроз кибератак для запугивания или принуждения государства, включая население страны, к продвижению навязываемых политических или социальных целей [Denning, 2000].

Однако кибертеррористы используют киберпространство не только для кибератак, но и для их планирования, подготовки, осуществления коммуникаций, получения финансирования, а также привлечения последователей, поскольку большое число террористических групп используют киберпространство для распространения своих идей [Hoffman, Schweitzer, 2015].

Заключение

Угроза, которую представляет кибертерроризм, становится все серьезнее. Развитие компьютерных и телекоммуникационных технологий происходит с невероятной скоростью, что требует более проницательного подхода к проблеме. Для того чтобы международные и национальные правоохранительные органы могли более эффективно бороться с кибертерроризмом, представляется, что необходимо более четкое понимание данного противозаконного явления. Для этого требуется единое законодательно закрепленное определение кибертерроризма, которое было бы общепринятым и применялось во всех правовых актах России, а также имело для общего толкования кибертерроризма и в международном праве.

Для определения кибертерроризма необходима оценка масштабов и механизмов террористической деятельности в киберпространстве всем мировым сообществом с учетом современного положения дел, с целью разработки таких мер правового регулирования, обеспечение которых в полной мере способствовали борьбе с кибертеррористами.

Это позволило бы унифицировать подходы к преследованию и наказанию кибертеррористов, а также облегчило бы обмен информацией и сотрудничество между правоохранительными органами разных стран.

Кроме того, необходимо учитывать быстрое развитие технологий и адаптировать правовую базу к новым угрозам. Кибертеррористы постоянно совершенствуют свои методы, поэтому правовая база должна быть гибкой и способной быстро реагировать на изменения в киберпространстве.

Важно также обратить внимание на международное сотрудничество в борьбе с кибертерроризмом. Такие преступления часто имеют трансграничный характер, и только совместные усилия могут привести к успешной борьбе с ними.

Необходимо развивать международные механизмы сотрудничества, обмена информацией и опытом, чтобы эффективно противостоять кибертеррористам в глобальном масштабе. Таким образом, разработка правовой базы и установление единого определения кибертерроризма являются неотъемлемыми шагами для эффективной борьбы с этой угрозой. Постоянное обновление и совершенствование правовой базы, а также укрепление международного сотрудничества помогут справиться с растущей угрозой кибертерроризма и обеспечить безопасность в киберпространстве.

Библиография

1. Агабалаев М. Правовой режим обеспечения общественной безопасности Российской Федерации. М., 2009. С. 5.
2. Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6. С. 167-177.
3. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. 2019. № 4 (91). С. 78-82.
4. Израильские хакеры вызвали массовые сбои в электросети Ирана. URL: https://www.securitylab.ru/news/542841.php?ysclid=lp16a1mnp23309229&utm_referrer=https%3A%2F%2Fya.ru%2F
5. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 31.03.2021) «Об утверждении государственной программы Российской Федерации «Информационное общество».
6. Сайт и приложение РЖД подверглись массированной хакерской атаке. URL: https://ria.ru/20230705/rzhd-1882317620.html?ysclid=lp14euibrl568822167
7. Самые крупные кибератаки 2023 года. URL: https://blog.cortel.cloud/2023/ 09/14/samye-krupnye-kiberataki-2023-goda/?ysclid=lp142jsjv2503011280
8. Указ Президента РФ от 01.12.2016 № 642 (ред. от 15.03.2021) «О Стратегии научно-технологического развития Российской Федерации».
9. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
10. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».
11. Denning D.E. Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University, 2000. URL: https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
12. Hoffman A., Schweitzer Y. Cyber Jihad in the Service of the Islamic State (ISIS). 2015. URL: https://www.inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf

Features of legal protection of the information and digital space of modern Russia in the conditions of information warfare

Nikita A. Mikhalenko

Postgraduate,
Samara State University of Economics,
443090, 141, Sovetskoi Armii str., Samara, Russian Federation;
e-mail: bote2018@gmail.com

Abstract

The author examines the current problems of the world community as a whole, and in particular Russia, related to such a type of cybercrime as cyberterrorism. Cyberterrorism, characterized by a high level of latency, as well as its scale and consequences, poses a threat to the information and digital space not only in modern Russia, but also for other countries. The author notes that currently there is a purposeful and coordinated nature of cyberattacks, so their danger of cyberattacks lies in the fact that cyberterrorists can attack even the automatic control systems of infrastructure facilities. The author deduces the causes of cyberterrorism, and also concludes that an effective fight against cyberterrorism requires the development of an appropriate legal framework that would define the concept of cyberterrorism and its criminal legal characteristics. This legal framework must constantly and dynamically develop due to the rapid development of information and digital technologies, and must also adapt to new threats. Developing a legal framework and establishing a common definition of cyberterrorism are integral steps to effectively combat the threat of cyberterrorism. Continuous updating and improvement of the legal framework, as well as strengthening international cooperation, will help cope with the growing threat of cyber terrorism and ensure security in cyberspace.

For citation

Mikhalenko N.A. (2023) Osobennosti pravovoi okhrany informatsionno-tsifrovogo prostranstva sovremennoi Rossii v usloviyakh informatsionnoi voiny [Features of legal protection of the information and digital space of modern Russia in the conditions of information warfare]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (11A), pp. 32-38. DOI: 10.34670/AR.2024.24.13.004

Keywords

Information and digital technologies, information security, cybercrime, cyberspace, cyberterrorism, cyberattacks, international community.

References

1. Agabalaev M. (2009) *Pravovoi rezhim obespecheniya obshchestvennoi bezopasnosti Rossiiskoi Federatsii* [Legal regime for ensuring public security of the Russian Federation]. Moscow.
2. Antonyan E.A., Aminov I.I. (2019) Blokchein-tekhnologii v protivodeistvii kiberterrorizmu [Blockchain technologies in countering cyberterrorism]. *Aktual'nye problemy rossiiskogo prava* [Current problems of Russian law], 6, pp. 167-177.
3. Buz S.I. (2019) Kiberprestupleniya: ponyatie, sushchnost' i obshchaya kharakteristika [Cybercrimes: concept, essence and general characteristics]. *Yurist-Pravoved* [Lawyer – Legal Scientist], 4 (91), pp. 78-82.
4. Denning D.E. (2000) *Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*. Georgetown University. Available at: https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html [Accessed 12/12/2023]
5. Hoffman A., Schweitzer Y. (2015) *Cyber Jihad in the Service of the Islamic State (ISIS)*. Available at: https://www.inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf [Accessed 12/12/2023]
6. *Izrail'skie khakery vyzvali massovye sboi v elektroseti Irana* [Israeli hackers caused massive outages in Iran's power grid]. Available at: https://www.securitylab.ru/news/542841.php?ysclid=lp16a1mnp23309229&utm_referrer=https%3A%2F%2Fya.ru%2F [Accessed 12/12/2023]
7. *Postanovlenie Pravitel'stva RF ot 15.04.2014 № 313 (red. ot 31.03.2021) «Ob utverzhdenii gosudarstvennoi programmy Rossiiskoi Federatsii «Informatsionnoe obshchestvo»* [Decree of the Government of the Russian Federation dated April 15, 2014 No. 313 (as amended on March 31, 2021) "On approval of the state program of the Russian Federation

"Information Society"].
8. *Sait i prilozhenie RZhD podverglis' massirovannoi khakerskoi atake* [The Russian Railways website and application were subject to a massive hacker attack]. Available at: https://ria.ru/20230705/rzhd-1882317620.html?ysclid=lp14euibrl568822167 [Accessed 12/12/2023]
9. *Samye krupnye kiberataki 2023 goda* [The biggest cyber attacks of 2023]. Available at: https://blog.cortel.cloud/2023/09/14/samye-krupnye-kiberataki-2023-goda/?ysclid=lp142jsjv2503011280 [Accessed 12/12/2023]
10. *Ukaz Prezidenta RF ot 01.12.2016 № 642 (red. ot 15.03.2021) «O Strategii nauchno-tekhnologicheskogo razvitiya Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation dated December 1, 2016 No. 642 (as amended on March 15, 2021) "On the Strategy for Scientific and Technological Development of the Russian Federation"].
11. *Ukaz Prezidenta RF ot 02.07.2021 № 400 «O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation dated July 2, 2021 No. 400 "On the National Security Strategy of the Russian Federation"].
12. *Ukaz Prezidenta RF ot 09.05.2017 № 203 «O Strategii razvitiya informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody»* [Decree of the President of the Russian Federation dated May 9, 2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030"].