ХАКТИВИЗМ КАК ФЕНОМЕН ТРАНСФОРМАЦИИ ГРАЖДАНСКОГО ПРОТЕСТА В ПОЛИТИЧЕСКИЙ ТЕРРОРИЗМ В КИБЕРПРОСТРАНСТВЕ

Айнутдинова К.А., *канд. юрид. наук, доцент,*
Университет управления «ТИСБИ», г. Казань;
Айнутдинова И.Н., *д-р пед. наук, профессор, ИМО КФУ, г. Казань*

Аннотация. Цель статьи - проанализировать феномен хактивизма с позиции трансформации его форм, стратегий, мотивов, моделей и методов в условиях геополитической нестабильности и экономической неопределенности. На основе изучения и анализа тематической литературы были выявлены современные тенденции хактивизма (организованность, структурированность, транснациональный характер, трансформация мотивов, связь с государством); установлены специфические признаки хактивизма; определены методы совершения хактивистских атак; проведено сравнение квалификации кибератак хактивистов с киберпреступлениями по УК РФ.

Abstract. The purpose of the article is to analyze the phenomenon of hacktivism from the perspective of transformation of its forms, strategies, motives, models and methods in conditions of geopolitical instability and economic uncertainty. Based on the study and analysis of thematic literature, modern trends in hacktivism were identified (organization, structure, transnational nature, transformation of motives, connection with the state); specific signs of hacktivism have been established; methods for carrying out hacktivist attacks have been identified; a comparison was made of the qualifications of cyberattacks by hacktivists with cybercrimes under the Criminal Code of the Russian Federation.

Ключевые слова: хактивизм, кибератака, киберпространство, гражданский протест, кибертерроризм.

Key words: hacktivism, cyberattack, cyberspace, civil protest, cyberterrorism.

Обращение к теме исследования вызвано ростом сообщений в СМИ о резонансных хакерских атаках, исходящих от различных организованных групп, ставящих целью привлечение внимания общественности к социальным, политическим и иным проблемам современности под лозунгом борьбы за «все хорошее против всего плохого», и направленных при этом на создание угроз объектам критической инфраструктуры, имуществу, жизни и здоровью людей [1]. Действуют эти группировки, именующие себя «хактивистами» (англ. *Hacktivists,* от слияния слов «хакер» и «активист»),

как правило, открыто и дерзко против всего, что противоречит их идеологии, взглядам и жизненным принципам [2]. Направляя свои атаки в киберпространстве против государственных структур, учреждений и политических деятелей, стратегически важных предприятий и организаций, они обычно делают упреждающие заявления и далее публикуют результаты своих акций в социальных сетях типа Twitter (X.), Facebook и др., размещают отчеты в YouTube, Blogspot или на специальных Telegram-каналах, а также активно используют скрытый сегмент Интернета Даркнет (англ. *DarkNet*), доступный только через специализированные браузеры (например, *Tor*), для коммуникации с сообщниками, группами поддержки и целевой аудиторией [3].

По мнению экспертов компаний, занимающихся защитой от киберугроз, таких как *Kaspersky* (Россия), *Cyberint* (Израиль), *Trellix, FireEye* (США) и др., сегодня отмечается небывалый всплеск хактивизма во всем мире, и к концу 2023 г. прогнозируется рост кибератак хактивистских групп как минимум на 11%. Происходит это в условиях, когда мировое сообщество переживает беспрецедентные времена геополитической нестабильности и экономической неопределенности, отягощенные длительными региональными и локальными конфликтами, кризисом энергоснабжения, стремительно растущей инфляцией и разрушительными социально-экономическими последствиями пандемии Covid-19. Затяжной глобальный кризис, или «пермакризис» (от англ. *permanent* (постоянный) и *crisis* (кризис)) спровоцировал также значительные изменения в экосистеме киберпространства, определил новые тенденции, стратегии и модели деятельности хактивистских групп, их возможности, связи и мотивы [4].

При всей очевидности и остроте проблемы в российском законодательстве термин «хактивизм» до сих пор не определен, как и многие другие понятия, связанные с преступлениями в киберпространстве. Это является, на наш взгляд, существенным пробелом, который препятствует пониманию сути хактивизма и не позволяет квалифицировать деяния хактивистов с позиции закона. Для уточнения юридической природы данного явления обратимся к его трактовке в зарубежных источниках. Так, по мнению А. Самуэль (*Alexandra W. Samuel*) под хактивизмом понимается «ненасильственное использование незаконных или юридически спорных цифровых инструментов для достижения политических целей» [5]. Шандор Вег (*Sandor Vegh*) рассматривает хактивизм [6] в качестве «политически мотивированного единичного действия в сети или связанной с ним кампанией, проводимой гражданскими субъектами, с целью выражения своего протеста, неодобрения и привлечения внимания общественности к поднимаемой проблеме».

М.Н. Марас (*Marie-Helen Maras*) описывает действия хактивистов как «преднамеренный доступ к системам, веб-сайтам и/или данным без

авторизации (…) в целях продвижения социальных или политических преобразований» [7]. Исходя из приведенных определений, можно предположить, что специфическими признаками хактивизма являются: ненасильственный характер действий акторов в киберпространстве; социально-политическая и идеологическая мотивированность участников; продвижение активной гражданской позиции и идей мирного протеста.

М.Н. Марас при этом достаточно критично описывает феномен хактивизма и ставит под сомнение его соответствие форме мирного политического протеста [7; 8]. Перечисляя методы хактивистов в киберпространстве, которые они используют для достижения своих целей и донесения некой «общественной позиции» на определенные события, автор указывает, что их действия де-факто подразумевают несанкционированный (незаконный) доступ к информационно-телекоммуникационных сетям, компьютерным системам, серверам, веб-сайтам и/или данным, являющимся объектами их атак, и влекут значительные разрушительные последствия [7]. По мнению М.Н. Марас, действия хактивистов, скорее, напоминают методы и технологии обычных киберпреступников, а не борцов за справедливость, действующих в рамках протестного движения [7; 8].

К наиболее распространенным методам хактивистов можно отнести: *дефейс* – взлом, порча и изменение содержимого атакованных веб-сайтов для публикации материалов, продвигающих идеи хактивистов; *редирект* – автоматическая переадресация пользователей с одного URL-адреса на другой веб-сайт; *DoS-атаки* – атаки типа «отказ в обслуживании» с целью блокировки или затруднения доступа обычных пользователей к ресурсам и сайтам; *DDoS-атаки* – распределенные атаки типа «отказ в обслуживании», проводимые одновременно с множества устройств и с подачей большого количества запросов, превышающих пропускную способность сети, с подключением зараженных «зомби-компьютеров» для блокировки работы сайта или ресурса жертвы с последующим вымогательством за остановку атаки в криптовалюте; *доксинг* – сбор конфиденциальной информации о человеке или организации с целью дальнейшего обнародования без его согласия; *Geo-bombing* – геобомбардировка с привязкой видеороликов на YouTube по определенной социальной или политической проблеме к конкретной точке (геотегу) на карте Google Earth. Хактивисты также не гнушаются и распространением вредоносных программ, кражей и раскрытием конфиденциальных данных, саботажем и пр. [3]. В РФ все перечисленные деяния квалифицируются как преступления в сфере компьютерной информации (ст.ст. 272-273 УК РФ), представляют общественную опасность [9] и не соответствуют понятию «мирный гражданский протест» [8].

Анализ литературы по теме исследования показал, что в предыдущие десятилетия хактивизм, действительно, воспринимался многими как форма

мирного гражданского протеста, выражаемая отдельными людьми или некими сообществами активистов, использующих свои компьютерные знания и навыки в программировании для социально обусловленного хакинга и продвижения конкретной социально-политической повестки без извлечения материальной выгоды [3]. В целом, такие акты гражданского протеста в сети «Интернет» не представляли значительных глобальных рисков, не порождали чувства тревоги, подавленности и страха у населения, а зачастую, наоборот, вызывали общественную поддержку, так как были направлены, несмотря на применение незаконных хакерских методов, инструментов и технологий, против нарушений прав человека, свободы слова, свободы распространения информации, любой несправедливости властей, уязвимостей в системе безопасности и пр. [2; 3; 7; 8].

Сегодня же, по мнению экспертов *Cyberint*, мы наблюдаем трансформацию хактивизма, который становится более организованным, структурированным и изощренным, а действия его акторов наносят непоправимый ущерб критической инфраструктуре и экономике государств. Это ведет к состоянию подавленности, угнетения и страха у больших групп людей из-за продолжительных опасных ситуаций, что, в итоге, сродни результатам реальных террористических актов [10]. Такие деяния могут быть квалифицированы как неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ); публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ); создание и/или участие в террористическом сообществе (чч. 1-2 ст. 205.4 УК РФ) [9; 10]. Примером хактивистской группы террористической направленности является украинская IT-армия, созданная по инициативе Минобороны Украины в 2022 г. и фактически легализованная государством; она имеет разветвленную сеть, куда входят такие ячейки, как *Anonymous, Cyber Partisans, AgainstTheWest, NB65* и др. Цели и задачи IT-армии включают информационно-психологические операции против населения России, организацию и проведение массированных DDoS-атак на государственные органы, ключевые инфраструктурные объекты и отрасли РФ, что, по мнению злоумышленников, должно привести к запугиванию населения, дестабилизации экономической, социальной и политической устойчивости в РФ.

Беспокойство вызывает сегодня и то, что многие хактивистские группы, известные ранее кибератаками по идеологическим мотивам, объединяются в транснациональные сообщества и сотрудничают с киберпреступниками в рамках противоправных деяний для извлечения финансовой выгоды. Новые тенденции по сплочению, усложнению структуры и сдвигу в сторону финансовой мотивации демонстрируют сегодня некоторые известные группировки. Например, Telegram-канал *Five*

Families представляет хорошо организованную взаимосвязанную сеть из различных ранее разрозненных хактивистских ячеек: *ThreatSec, GhostSec*, *Stormous, Blackforums* и *SiegedSec*. Аналогичным образом, *Anonymous Sudan* из Судана строит партнерские отношения с другими группировками типа *REvil* и *KillNet* для усиления своих возможностей по реализации киберугроз и нанесению финансового ущерба таким крупным корпорациям, как *Microsoft* и *Riot Games*. С учетом того, что для достижения своих целей хактивисты используют методы и технологии киберпреступников, сдвиг в сторону финансовой мотивации ставит их в один ряд с обычными хакерами, то есть лицами, совершающими преступления в сфере компьютерной информации (ст.ст. 159.6, 272, 273, 274 УК РФ) [9; 10].

Еще одна тенденция прослеживается в связях хактивистских группировок с государственными структурами, с формированием четкой политической повестки, в следовании госзаказу и служении особым интересам конкретных правительств, что также знаменует собой эволюцию методов их работы. Известно, что связанная с Россией группа *SiegedSec* провела в этом году эффективные атаки на серверы НАТО и крупнейшую компанию-разработчика программного обеспечения из Австралии *Atlassian*, что свидетельствует о растущей смелости операций хактивистов и их способности бросать вызов крупным организациям. Другая российская хак-группа - *KillNet* еще в апреле 2023 г. атаковала Европейскую организацию по безопасности воздушной навигации (Евроконтроль), имеющую тесные связи с блоком НАТО, а в октябре 2023 г. провела еще одну серьезную DDoS-атаку уже на авиакомпании США. Действия взломщиков привели к простою сайтов 14-ти авиакомпаний, что нарушило доступ пассажиров к ресурсам, информирующим о загруженности аэропортов и времени ожидания рейсов. При этом отмечается, что киберинциденты не затронули управление воздушным движением, транспортную безопасность и линии связи с самолетами [1].

Исследование малоизученного феномена хактивизма, его сложной сетевой структуры, новых тенденций, стратегий и моделей деятельности хактивистских групп позволило нам по-новому взглянуть на быстроменяющийся ландшафт киберпространства и глобальные угрозы кибербезопасности, таящиеся в нем [3]. Нами было установлено, что небывалый всплеск хактивизма во всем мире обусловлен сегодня, в большей степени, факторами затяжной геополитической нестабильности и экономической неопределенности, что повлекло, в том числе, значительные изменения в экосистеме киберпространства, расширило способы и методы совершения киберпреступлений и осложнило способы борьбы с ними. Активность хактивистов, вероятно, продолжит расти и в будущем, а риску будут подвергаться не только правительства и организации, участвующие в региональных и локальных конфликтах. Как показывает мировая практика,

любая политическая или социальная проблема может спровоцировать деятельность хактивистов, а это означает, что любое государство, независимо от размера и уровня развития, как и любая организация, независимо от отрасли и ее значимости, потенциально могут стать мишенью хактивистов. Не случайно вопросы обеспечения информационной и кибербезопасности приобретают сегодня особое значение, при этом важно быть в курсе текущих геополитических ситуаций, которые могут усиливать эти угрозы.

Литература:

1. Romagna, M. & Leukfeldt, R.E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism // Journal of Crime and Justice. - Pp. 1-19. - DOI: 10.1080/0735648X.2023.2216189.

2. Самуэль, А.В. Феномен хактивизма // Политич. наука. - 2008. - № 2. - С. 119-131.

3. Romagna, M. (2019). Hacktivism: Conceptualization, Techniques and Historical View // In: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. - Pp. 1-27. - DOI: 10.1007/978-3-319-90307-1_34-1.

4. Goes, C. & Bekkers, E. (2022). The Impact of Geopolitical Conflicts on Trade, Growth, and Innovation / Carlos Goes; Eddy Bekkers. UC San Diego, World Trade Organization. - Pp. 1-59.

5. Samuel, A. (2004). Hacktivism and the Future of Political Participation. - Cambridge, Massachusetts: Harvard University. - 284 p.

6. Vegh, S. (2003). Hacking for Democracy: A Study of the Internet as a Political Force and Its Representation in the Mainstream Media. - University of Maryland, College Park. – 698 p.

7. Maras, M. (2016). Cybercriminology / Marie-Helen Maras. - Oxford University Press. - 448 p.

8. Михайлова, Е.В., Скогорев, А.П. Протесты как форма гражданской активности в современной России // Власть. - 2017. - № 1. - С. 54-59.

9. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 12.10.2023). [Электрон. ресурс]. - Дата доступа: 27.10.2023. - URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.

10. Прудникова, К.К., Бондаренко Н.А. Терроризм в эпоху информационных технологий // Уральский ж-л правовых исслед. - 2022. - № 2. - С. 74-80. - DOI 10.34076/2658_512X_2022_2_74.