ПОЛИТОЛОГИЯ

УДК 327

ХАКТИВИЗМ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ ВОЙНЫ: ОПЫТ РОССИЙСКО-УКРАИНСКОГО КОНФЛИКТА (2022–2023)

Д. А. Патрушева, В. В. Уласик

Попытка понять влияние хактивизма в разрешении и продолжении конфликта на Украине начиная с 2022 года. Обращается внимание на рост киберпреступности, а также на разнообразные сообщества хактивистов, активно участвующих в этом процессе. Приводятся конкретные случаи хакерских атак, произошедших после начала войны [1] в Украине, и их последствия. Анализ методов, таких как хакерские атаки, распространение киберпропаганды, и использование социальных сетей для мобилизации граждан и формирования общественного мнения. Демонстрируется, что хактивизм играет важную роль в информационной войне и используется для достижения политических целей.

Ключевые слова: хактивизм, Украинский конфликт, кибербезопасность, политические цели, кибератаки, информационная война, кибервойна, кибератаки, стратегии защиты информационных ресурсов.

Хактивизм, как форма активизма, использующая технологии информационной безопасности и киберпространства для достижения политических целей, играет значительную роль в современных конфликтах, включая тот, который происходит на Украине.

В период конфликта наблюдается также значительное увеличение киберпреступлений [2]. Кибератаки направлены как на государственные, так и на частные структуры, с целью дестабилизации обстановки, ослабления инфраструктуры и воздействия на общественное мнение. Эти атаки включают в себя распространение дезинформации, кибершпионаж, кибертерроризм, кибервандализм и другие формы агрессивной деятельности.

В открытом доступе не столь много информации о сообществах, известна лишь часть групп, которые не скрываются и признают свои преступления, а именно: в России это – “KillNet” [3], “Noname057(16)” [4], “Turla” [5], “APT28” (он же “Fancy Bear” с 2004-2007) [6], в Украине – “The IT Army of Ukraine” [7], на второй день войны публично объявлена Министерством Цифровой Трансформации Украины как создание IT-армии, которая в основном координирует свои усилия через “Telegram” и “Twitter” [8] (там они сообщают подписчикам данную информацию с просьбой о ее распространении в социальных сетях, в частности “ВКонтакте”, так как пользователей из России в ней превышает 91 миллионов человек) [9], “Cyber.Anarchy.Squad” [10], “Hack Your Mom” [11] – созданный коллективом хактивистов в Харькове, “Cyber.Unit Tech” [12], а также члены некоторых групп, которые впоследствии объединились, как, например, “Украинский кибераль янс” [13]. Другие волонтеры организуют и публикуют информацию и статьи, такие как “InformNapalm” [14]. Кроме того, хотелось бы отметить, что после начала войны к украинским хакерам присоединились белорусские хактивисты, а именно “Киберпартизаны” [15] с момента объявления антивоенной мобилизации, тем самым стремились «Парализовать работу государственной инфраструктуры, не вредя здоровью и жизням людей» [16].

Анализируя статистику за 2022 год, можно отметить, что количество кибератак на государственный сектор выросло в 2-3 раза по сравнению с 2021 годом [17].

По официальным данным, количество утечек конфиденциальной информации в российском госсекторе за 2022 г. выросло почти в 1,5 раза по сравнению с 2021 году. Кибератаки с целью хищения данных или полного разрушения IT-инфраструктуры резко выросло в первые девять месяцев 2023 года: на рекордные 140%. Киберугроз за январь – сентябрь увеличилось на 75% в сравнении с тем же периодом 2022 года [18]. В 2024 году число DDoS-атак на российский бизнес вырастет как минимум на 400% в связи с нестабильной политической ситуацией, следует из прогноза отдела кибербезопасности "EdgeЦентра" [19].

Рассматривая же Украину, то, по официальной информации, в 2022 году количество кибератак выросло почти втрое, чем в 2021 году. С начала 2023 года (по сравнению с 4 кварталом 2022-го) кибератак от пророссийских группировок стало меньше, но они систематичные и интенсивные [20]. Российские кибергруппы воспользовались для взлома известными им изъянами в защите приложения портала государственных услуг Украины "Дія" [21], чтобы получить доступ к данным о 2,6 млн. частных лиц, предприятий и юридических фирм, а также правительственных учреждений [22]. По подсчетам Госспецсвязи Украины, за 2023 год было обнаружено 1516861 подозрительных уникальных файлов, при этом чаще всего выявляли вирусы типа Smoke Loader, Agent Tesla, Snake Keylogger, Remcos, Formbook. Совершено 92 атаки на энергетический сектор, 81 случай – на телеком, 38 – образовательные учреждения, 32 – транспортную отрасль, 30 – финансовый сектор, 25 – IT-сектор, 15 – СМИ, 12 – медицинские учреждения [23]. В 2024 году прогнозируют, что Украина будет сталкиваться с более сложными кибератаками, к которым Россия будет привлекать ИИ, об этом сообщил специалист Правительственной команды реагирования на компьютерные чрезвычайные события Украины CERT-UA Назар Тимошик во время выступления на конференции SANS CyberThreat 2023 году [24].

Рассмотрим наиболее известные инциденты взлома, произошедшие начиная с 24 февраля 2022 года:

С 24 по 28 февраля 2022 число хакерских атак на российские компании, госорганы, банки и СМИ выросло как минимум втрое, а также возможны утечки сервисов – данные от "Лаборатории Касперского" [25] (2022);

Взлом сайта Минфина Украины (2022) – удалось получить доступ к почтам сотрудников ведомства, а также изъять более миллиона файлов с электронными документами [26];

Взлом эфира "Украина 24" и демонстрация фейкового заявления Зеленского (2022) – в прямом эфире телеканала «Украина-24» бегущей строкой появилось якобы обращение президента Владимира Зеленского сложить оружие всем военным и об уходе с поста. Президент Украины Зеленский немедленно опроверг фейковое заявление и назвал вмешательство провокацией [27];

Кибератака на Украинские правительственные сайты (2022) – в результате масштабной атаки были взломаны все 755 сайтов органов власти Украины [28];

Украинская разведка заявила, что взломала Федеральную налоговую службу России (2023) – в рамках операции хакерам удалось взломать центральный сервер ФНС, после чего спецслужбы получили доступ к более чем двум тысячам региональных серверов [29]. Вдобавок, хакерская атака затронула российскую IT-компанию, которая предоставляла услуги банка данных для ФНС, по информации, предоставленной ГУР. Представители ведомства утверждают, что в процессе операции "все серверы [ФНС] были заражены вредоносным программным обеспечением, а в результате кибератаки "были полностью уничтожены конфигурационные файлы, обеспечивающие работу распределенной системы ФНС". Кроме того, в ГУР сообщили, что база данных налоговой и ее резервные копии,

по их данным, были удалены. Представители ФНС отрицали факт взлома [30];

Атака на крупнейшего в Украине оператора связи «Киевстар» (2023) – сбой с помощью хакерской атаки на ядро сети [31]. Как позже отметил президент компании Александр Комаров: «Это самая большая в мире хакерская атака на телеком-инфраструктуру» [32];

Взлом сайта Киевского облсовета с угрожающим посланием Владимиру Зеленскому на русском языке (2023) – исполняющий обязанности главы совета Киевской области Ярослав Добрянский уточнил, что вместе с сайтом хакеры взломали серверы облсовета, из-за чего сотрудники не могут получить доступ к компьютерам, тем самым "работа аппарата фактически оказалась парализована" [33].

Все указанные инциденты демонстрируют размер киберугроз, с которыми сталкивается мир в эпоху цифровизации. Взломы, хакерские атаки и кибершпионаж превратились в неотъемлемый элемент современной геополитики, что подчеркивает критическое значение кибербезопасности как первоочередной задачи не только для государственных структур, но и для коммерческих организаций и обычных граждан.

Из этого можно сделать вывод, что невозможно выделить какую-то одну среди этих обеих стран и заявлять, что они совершают больше киберпреступлений, чем другая. Как Россия, так и Украина взламывает и опубликовывает персональные данные военных, и здесь следовало бы напомнить о женевской конвенции об обращении с военнопленными 1949 года – ключевой документ международного права, который устанавливает нормы и принципы, касающиеся обращения с военнопленными и их личных данных, во время вооруженных конфликтов. Раздел 2 конвенции включает в себя постановления общего характера о защите военнопленных. Статья 12 этого раздела подчеркивает необходимость гуманного обращения с военнопленными. Запрещает любые незаконные действия или бездействие со стороны держащей в плену, которые могут привести к смерти или серьезному ущербу здоровью военнопленного. Кроме того, запрещает физическое калечение военнопленных или их использование в качестве объектов научных или медицинских экспериментов без их согласия. Вместе с тем гарантирует защиту военнопленных от насилия, запугивания, оскорблений и любопытства толпы. Применение к ним репрессалий также запрещается [34]. Тем не менее, как СМИ, так и отдельные граждане играют свою роль в соблюдении данных стандартов.

Проведённое исследование организацией Check Point Research (CPR) [35] в 2023 году подчеркнуло, что сентябрь 2022 года стал поворотным моментом в кибератаках, связанных с конфликтом. Если сравнивать март – сентябрь 2022 года с октябрем 2022 года – февралем 2023 года, то CPR выявил снижение на 44% среднего количества еженедельных атак на одну организацию против Украины, с 1555 атак до 877, увеличение среднего числа еженедельных атак на Российскую Федерацию на одну организацию на 9%, с 1505 до 1635 соответственно. Исходя из статистических данных, CPR показывает, что начиная с октября 2022 года произошел сдвиг в кибератаках, связанных с войной, в то время как гораздо больше усилий в киберпространстве сейчас направлено на страны НАТО, чем на Украину.

Check Point Research: CPR представили данные, где указано среднее количество еженедельных кибератак на одну организацию правительства и военной промышленности начиная с сентября 2022 года (Рис.1).

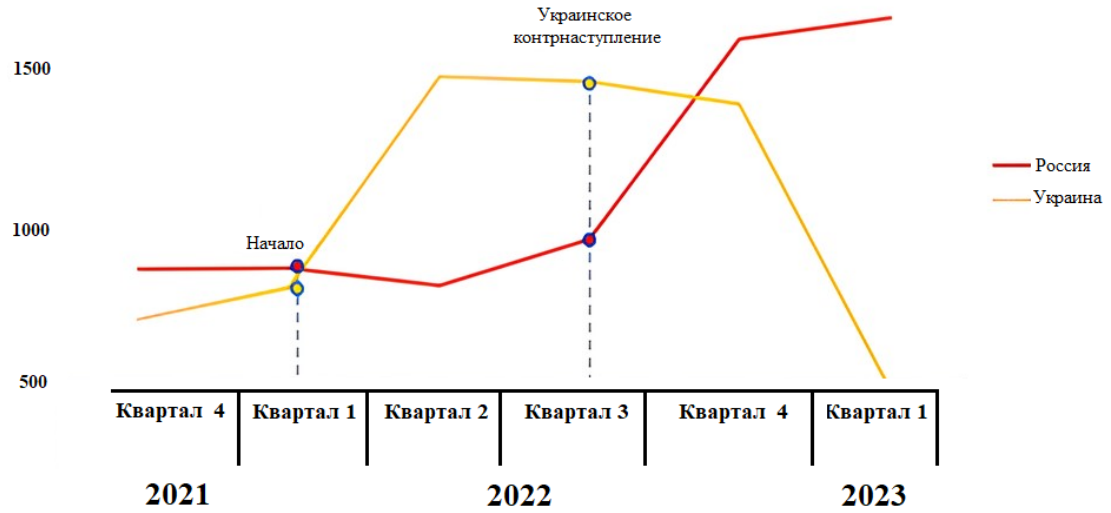

Рис. 1 - Среднее количество еженедельных кибератак на одну организацию.

MDPI провело исследование «Аналитика социальных сетей о Российско–Украинской кибервойне с использованием обработки естественного языка» [36], где была представлена диаграмма с указанием среднемесячного негативного настроя российских и украинских пользователей, связанных с кибербезопасностью, и сравнивали их с общемировыми показателями (Рис. 2).

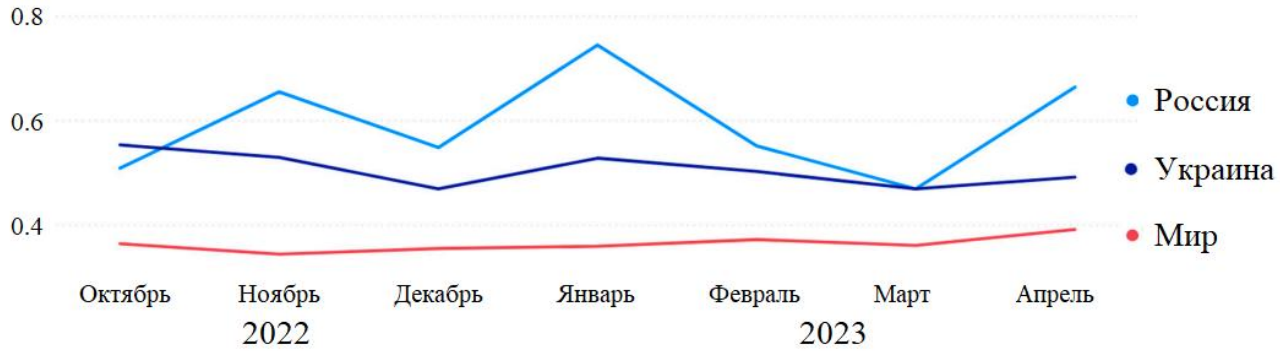

Рис. 2. Среднемесячный негативный настрой российских и украинских пользователей.

Попытка обнаружить статистические данные относительно количества киберпреступлений, совершенных со стороны Украины в отношении России, оказалась безуспешной, поскольку доступна только официальная статистика, касающаяся киберпреступлений, совершенных со стороны России в отношении Украины.

Стоит отметить, что хактивизм в контексте Украинского конфликта выступает важным элементом информационной войны. Повышение уровня киберпреступности и активности хактивистов как в отношении государственных, так и частных структур свидетельствует о том, что киберпространство становится основной ареной для борьбы, а также средством достижения политических целей.

Различные хактивистические группы России и Украины, активно участвуют в этом процессе, что привносит сложности в геополитическую ситуацию. Важно подчеркнуть, что такие действия могут иметь серьезные последствия не только для государственных структур, но и для обычных граждан, что подчеркивает необходимость развития механизмов кибербезопасности. Кроме того, необходимо активно развивать технические средства защиты информации и сетевых систем, в том числе разрабатывать новые методы обнаружения и предотвращения киберугроз, повышать квалификацию специалистов в области кибербезопасности и содействовать развитию инновационных технологий в этой области. Эф-

фективное противодействие требует не только технических и правовых мер, но и международного сотрудничества и координации действий всех заинтересованных сторон. Только совместные усилия на региональном, национальном и международном уровнях позволят эффективно противодействовать угрозам в киберпространстве и обеспечить стабильность и безопасность как национальной, так и глобальной информационной среды.

Список источников и литературы

1. *Алиев Н.* Кибероперации в ходе российского вторжения в Украину в 2022 году / Н. Алиев [Электронный ресурс] // Riddle Russia: [сайт]. — URL: https://ridl.io/ru/kiberoperatsii-v-hode-rossijskogo-vtorzheniya-v-ukrainu-v-2022-godu/ (дата обращения: 18.10.2024)

2. *Баласян Л.* Edge Центр спрогнозировал рост кибератак на бизнес на 400% в 2024 году / Л. Баласян [Электронный ресурс] // Forbes: [сайт]. — URL: https://www.kommersant.ru/doc/6425423 (дата обращения: 15.10.2024)

3. *Бегаль И.* В 2022 году количество кибератак на Украину выросло почти втрое. 90% хакерских групп из РФ контролируют силовики / И. Бегаль [Электронный ресурс] // Forbes: [сайт]. — URL: https://forbes.ua/ru/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата обращения: 12.10.2024)

4. *Ворошилов Д.* Бегущую строку «Украины 24» взломали и разместили сообщение о капитуляции / Д. Ворошилов [Электронный ресурс] // РБК: [сайт]. — URL: https://www.rbc.ru/politics/16/03/2022/6231c8049a79475eebf30dc4 (дата обращения: 15.10.2024)

5. Группа хакеров сообщила о взломе портала украинского минфина / [Электронный ресурс] // Известия: [сайт]. — URL: https://iz.ru/1429248/2022-11-22/gruppa-khakerov-soobshchila-o-vzlome-portala-ukrainskogo-minfina (дата обращения: 15.10.2024)

6. Женевская конвенция от 12 августа 1949 года об обращении с военнопленными / [Электронный ресурс] // United Nations: [сайт]. — URL: https://www.un.org/ru/documents/decl_conv/conventions/geneva_prisoners_2.shtml (дата обращения: 18.10.2024)

7. *Злобин А.* Песков заявил о превращении «спецоперации» на Украине в «войну» / Злобин А. [Электронный ресурс] // Forbes : [сайт]. — URL: https://www.forbes.ru/society/508717-peskov-zaavil-o-prevrasenii-specoperacii-na-ukraine-v-vojnu (дата обращения: 15.10.2024)

8. *Калюков Е.* СБУ назвала катастрофой атаку хакеров на «Киевстар»: уничтожено почти всё / Е. Калюков [Электронный ресурс] // РБК: [сайт]. — URL: https://www.rbc.ru/politics/04/01/2024/659676a59a79475242966ec0 (дата обращения: 18.10.2024)

9. *Курашева А., Устинова А.* Хакеры атаковали госорганы в три раза чаще в 2022 году / А. Курашева, А. Устинова [Электронный ресурс] // Ведомости: [сайт]. — URL: https://www.vedomosti.ru/technology/articles/2023/01/16/959104-hakeri-atakovali-gosorgani-chasche (дата обращения: 15.10.2024)

10. *Мельник Т.* «Это самая большая в мире хакерская атака на телеком-инфраструктуру». Первое интервью президента «Киевстара» после кибератаки, парализовавшей оператора / Т. Мельник [Электронный ресурс] // Forbes: [сайт]. — URL: https://forbes.ua/ru/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855 (дата обращения: 12.10.2024)

11. *Мельник В.* Количество кибератак в Украине возросло: кто оказался под угрозой и какие вирусы использовали чаще всего / В. Мельник [Электронный ресурс] // Викна: [сайт]. — URL: https://vikna.tv/ru/dlia-tebe/bezpeka/kolichestvo-kiberatak-v-ukraine-za-2023-god-vozroslo/ (дата обращения: 15.10.2024)

12. Месячная активная аудитория VK ID за год выросла до 91 млн. пользователей / [Электронный ресурс] // ТАСС: [сайт]. — URL: https://tass.ru/ekonomika/18657631 (дата обращения: 15.10.2024)

13. *Наумова Е.* Сайты органов государственной власти Украины перестали работать из-за кибератаки / Е. Наумова [Электронный ресурс] // Lenta.ru: [сайт]. — URL: https://lenta.ru/news/2022/03/03/hackers_ukraine/ (дата обращения: 18.10.2024)

14. *Панасюк В.* В 2024 году россия планирует использовать ИИ для кибератак на Украину / В. Панасюк [Электронный ресурс] // Мета: [сайт]. — URL: https://meta.ua/news/tech/101946-v-2024-godu-rossiya-planiruet-ispolzovat-ii-dlya-kiberatak-na-ukrainu/ (дата обращения: 12.10.2024)

15. *Пламенев И.* В ФНС опровергли взлом налоговой системы украинской разведкой / И. Пламенев [Электронный ресурс] // РБК: [сайт]. — URL: https://www.rbc.ru/society/12/12/2023/657890839a79477f74b0c200 (дата обращения: 18.10.2024)

16. *Руденко М.* Хакеры взломали сайт Киевского облсовета / М. Руденко [Электронный ресурс] // РИА Новости: [сайт]. — URL: https://ria.ru/20231102/khakery-1907005140.html .

17. Светлана Тихановская объявила "антивоенную мобилизацию" / [Электронный ресурс] // Euronews: [сайт]. — URL: https://ru.euronews.com/2022/03/02/belarus-tsikhanowskaya-antiwar-mobilisation (дата обращения: 15.10.2024)

18. *Степанова Ю., Исакова Т.* Утечки получили подкрепление / Ю. Степанова, Т. Исакова [Электронный ресурс] // Коммерсантъ: [сайт]. — URL: https://www.kommersant.ru/doc/5240325 (дата обращения: 15.10.2024)

19. *Таиров Р.* Бывшая Group-IB заявила о рекордном росте кибератак по политическим мотивам / Р. Таиров [Электронный ресурс] // Forbes: [сайт]. — URL: https://www.forbes.ru/tekhnologii/498860-byvsaa-group-ib-zaavila-o-rekordnom-roste-kiberatak-po-politiceskim-motivam (дата обращения: 15.10.2024)

20. *Тейзе К., Шварц Я.* Как белорусские "киберпартизаны" помогают Украине на войне / К. Тейзе. Я. Шварц [Электронный ресурс] // DW: [сайт]. — URL: https://www.dw.com/ru/belorusskie-kiberpartizany-pomogajut-ukraine-v-vojne-s-rossiej/a-62237250 (дата обращения: 18.10.2024)

21. *Чикишев Н.* Украинская разведка заявила о взломе российской налоговой. Вся база якобы уничтожена / Н. Чикишев [Электронный ресурс] // devby.io: [сайт]. — URL: https://devby.io/news/ukrainskaya-razvedka-zayavila-o-vzlome-rossiiskoi-nalogovoi-vsya-baza-yakoby-unichtozhena (дата обращения: 15.10.2024)

22. Antoniuk D. Pro-Ukraine hackers claim to take down Russian internet provider / Daryna Antoniuk [Electronic Resource] // The Record from Recorded Future News: [site]. — URL: https://therecord.media/proukraine-hackers-claim-to-take-down-russian-isp (last request: 15.10.2024)

23. Check Point Research Team. The Russian-Ukrainian War, One Year Later / Check Point Research Team [Electronic Resource] // Check Point Blog: [сайт]. — URL: https://blog.checkpoint.com/2023/02/21/the-russian-ukrainian-war-one-year-later/ (last request: 18.10.2024)

24. 'Diya' personal data leak: Ukraine's Digital Transformation Ministry called out over social media manipulation and use of bots / [Electronic Resource] // https://mezha.net/: [site]. — URL: https://mezha.net/eng/bukvy/diya-personal-data-leak-ukraine-s-digital-transformation-ministry-called-out-over-social-media-manipulation-and-use-of-bots/ (last request: 15.10.2024)

25. *Gajos W.* How Russia's NoName057(16) could be a new model for hacking groups / Wiktoria Gajos [Electronic Resource] // CSO Online : [site]. — URL: https://www.csoonline.com/article/1270051/how-russias-noname05716-could-be-a-new-model-for-hacking-groups.html (last request: 12.10.2024)

26. *Huntley S.* Fog of war: how the Ukraine conflict transformed the cyber threat landscape / Shane Huntley [Electronic Resource] // Google Blog: [site]. — URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (last request: 15.10.2024)

27. Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective / [Electronic Resource] // FLASHPOINT: [site]. — URL: https://flashpoint.io/intelligence-101/killnet/ (last request: 18.10.2024)

28. *McLaughlin J.* Ukrainian hackers and intel officers partner up in apparent hack of a top Russian bank / Jenna McLaughlin [Electronic Resource] // NPR: [site]. — URL: https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (last request: 15.10.2024)

29. *McLaughlin J.* Ukrainian hacktivists fight back against Russia as cyber conflict deepens / Jenna McLaughlin [Electronic Resource] // NPR: [сайт]. — URL: https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war (last request: 15.10.2024)

30. *Pearson J.* Ukraine launches 'IT army,' takes aim at Russian cyberspace / James Pearson [Electronic Resource] // Reuters: [site]. — URL: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/ (last request: 15.10.2024)

31. *Render-Katolik A.* The IT Army of Ukraine / Aiden Render-Katolik [Electronic Resource] // CSIS | Center for Strategic and International Studies: [site]. — URL: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine (last request: 18.10.2024)

32. *Sayegh E.* Turla Hacking Group: A Persistent International Threat / Emil Sayegh [Electronic Resource] // Forbes: [site]. — URL: https://www.forbes.com/sites/emilsayegh/2023/03/07/turla-hacking-group-a-persistent-international-threat/?sh=b888ef574980 (last request: 12.10.2024)

33. *Sayegh E.* APT28 Aka Fancy Bear: A Familiar Foe By Many Names / Emil Sayegh [Electronic Resource] // Forbes: [site]. — URL: https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/?sh=6349519059ad (last request: 15.10.2024)

34. *Sufi F.* Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges / Fahim Sufi [Electronic Resource] // MDPI: [site]. — URL: https://www.mdpi.com/2078-2489/14/9/485 (last request: 15.10.2024)

35. Supruniuk I., Aushev Y. CyberUnit.Tech & Cyber School: “Our mission is to elevate the perception of Ukraine as a country of innovation” / Iryna Supruniuk [Electronic Resource] // TechUkraine: [site]. — URL: https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (last request: 12.10.2024)

36. Srishti Singh Sisodia. Using fake profiles of women, Ukrainian hackers duped Russian soldiers to help military: Report / Srishti Singh Sisodia [Electronic Resource] // WION: [site]. — URL: https://www.wionews.com/world/using-fake-profiles-of-women-ukrainian-hackers-duped-russian-soldiers-to-help-military-report-513399 (last request: 15.10.2024)

Патрушева Дарья Андреевна – старший преподаватель кафедры истории и регионоведения, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (г. Санкт-Петербург, Россия), d.patrusheva@mail.ru

Уласик Вероника Валерьевна – студентка 3 курса бакалавриата, направления системное и прикладное программирование информационных систем, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (г. Санкт-Петербург, Россия), nika.ulasik@gmail.ru

HACKTIVISM IN THE CONTEXT OF INFORMATION WAR: THE EXPERIENCE OF THE RUSSIAN-UKRAINIAN CONFLICT (2022–2023)

D. A. Patrusheva, V. V. Ulasik

An attempt to understand the impact of hacktivism on the resolution and continuation of the conflict in Ukraine since 2022 is made. Attention is drawn to the growth of cybercrime, as well as various communities of hacktivists actively involved in this process. Specific cases of hacker attacks that occurred after the beginning of the war [1] in Ukraine and their consequences are presented. The analysis of methods such as hacker attacks, the spread of cyber propaganda, and the use of social networks for mobilizing citizens and shaping public opinion is provided. It is demonstrated that hacktivism plays an important role in the information war and is used to achieve political goals.

Keywords: hacktivism, Ukrainian conflict, cybersecurity, political goals, cyber attacks, information war, cyber war, cyber attacks, strategies for protecting information resources.

References

1. *Aliyev N.* Kiberoperatsii v khode rossiyskogo vtorzheniya v Ukrainu v 2022 godu [Cyber Operations During the Russian Invasion of Ukraine in 2022] / N. Aliyev [Electronic resource] // Riddle Russia: [website]. — URL: https://ridl.io/ru/kiberoperatsii-v-hode-rossijskogo-vtorzheniya-v-ukrainu-v-2022-godu/ (last request: 18.10.2024) (In Russ)

2. *Balyasyan L.* EdgeTsentr sprognoziroval rost kiberatak na biznes na 400% v 2024 godu [EdgeCenter Forecasts a 400% Increase in Cyber Attacks on Businesses in 2024] / L. Balyasyan [Electronic resource] // Forbes: [website]. — URL: https://www.kommersant.ru/doc/6425423_(last request: 15.10.2024) (In Russ)

3. *Begal I.* V 2022 godu kolichestvo kiberatak na Ukrainu vyroslo pochti vtroe. 90% khakerskikh grup iz RF kontroliruyut siloviki [In 2022, the Number of Cyber Attacks on Ukraine Almost Tripled. 90% of Russian Hacker Groups are Controlled by Law Enforcement]/ I. Begal [Electronic resource] // Forbes: [website]. — URL: https://forbes.ua/ru/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (last request: 12.10.2024) (In Russ)

4. *Voroshilov D.* Begushchuyu stroku «Ukrainy 24» vzlomali i razmestili soobshchenie o kapitulyatsii [Ukraine 24's Ticker Hacked, Message About Capitulation Posted] / D. Voroshilov [Electronic resource] // RBC: [website]. — URL: https://www.rbc.ru/politics/16/03/2022/6231c8049a79475eebf30dc4 (last request: 15.10.2024) (In Russ)

5. Gruppa khakerov soobshchila o vzlome portala ukrainskogo minfina [Hacker Group Reports Hacking of Ukrainian Ministry of Finance Portal] / [Electronic resource] // Izvestia: [website]. — URL: https://iz.ru/1429248/2022-11-22/gruppa-khakerov-soobshchila-o-vzlome-portala-ukrainskogo-minfina (last request: 15.10.2024) (In Russ)

6. Zhenevskaya konventsiya ot 12 avgusta 1949 goda ob obrashchenii s voennoplennymi [Geneva Convention of August 12, 1949 on the Treatment of Prisoners of War] / [Electronic resource] // United Nations: [website]. — URL: https://www.un.org/ru/documents/decl_conv/conventions/geneva_prisoners_2.shtml (last request: 18.10.2024) (In Russ)

7. *Zlobin A.* Peskov zayavil o prevrashchenii «spetsoperatsii» na Ukraine v «voynu» [Peskov Announced the Transformation of the "Special Operation" in Ukraine into a "War"] / A. Zlobin [Electronic resource] // Forbes: [website]. — URL: https://www.forbes.ru/society/508717-peskov-zaavil-o-prevrasenii-specoperacii-na-ukraine-v-vojnu (last request: 15.10.2024) (In Russ)

8. *Kalyukov E.* SBU nazvala katastrofoy ataku khakerov na «Kievstar»: unichtozheno pochti vsyo [The Security Service of Ukraine Called the Hacker Attack on Kyivstar a Disaster: Almost Everything Was Destroyed] / E. Kalyukov [Electronic resource] // RBC: [website]. — URL: https://www.rbc.ru/politics/04/01/2024/659676a59a79475242966ec0 (last request: 18.10.2024) (In Russ)

9. *Kurasheva A.,* Ustinova A. Khakery atakovali gosorgany v tri raza chashche v 2022 godu [Hackers Attacked Government Agencies Three Times More Often in 2022] / A. Kurasheva, A. Ustinova [Electronic resource] // Vedomosti: [website]. — URL: https://www.vedomosti.ru/technology/articles/2023/01/16/959104-hakeri-atakovali-gosorgani-chasche (last request: 15.10.2024) (In Russ)

10. *Melnik T.* «Eto samaya bol'shaya v mire khakerskaya ataka na telekom-infrastrukturu». Pervoye interv'yu prezidenta «Kievstara» posle kiberataki, paralizovavshey operatora ["This is the Largest Cyber Attack on Telecom Infrastructure in the World." First Interview of Kyivstar's President After Cyber Attack That Paralyzed the Operator] / T. Melnik [Electronic resource] // Forbes: [website]. — URL: https://forbes.ua/ru/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855 (last request: 12.10.2024) (In Russ)

11. *Melnik V.* Kolichestvo kiberatak v Ukraine vozroslo: kto okazalsya pod ugrozoy i kakie virusy ispol'zovali chashche vsego [The Number of Cyber Attacks in Ukraine Has Increased: Who is at Risk and What Viruses Were Most Often Used] / V. Melnik [Electronic resource] // Vikna: [website]. — URL: https://vikna.tv/ru/dlia-tebe/bezpeka/kolichestvo-kiberatak-v-ukraine-za-2023-god-vozroslo/ (last request: 15.10.2024) (In Russ)

12. Mesyachnaya aktivnaya auditoriya VK ID za god vyrosla do 91 mln pol'zovateley [VK ID Monthly Active Audience Grew to 91 Million Users Over the Year] / [Electronic resource] // TASS: [website]. — URL: https://tass.ru/ekonomika/18657631 (last request: 15.10.2024) (In Russ)

13. *Naumova E.* Sayty organov gosudarstvennoy vlasti Ukrainy perestali rabotat' iz-za kiberatak [Ukrainian Government Websites Stopped Working Due to Cyber Attack] / E. Naumova [Electronic resource] // Lenta.ru: [website]. — URL: https://lenta.ru/news/2022/03/03/hackers_ukraine/ (last request: 18.10.2024) (In Russ)

14. *Panasyuk V.* V 2024 godu Rossiya planiruet ispol'zovat' II dlya kiberatak na Ukrainu [In 2024, Russia Plans to Use AI for Cyber Attacks on Ukraine] / V. Panasyuk [Electronic resource] // Meta: [website]. — URL: https://meta.ua/news/tech/101946-v-2024-godu-rossiya-planiruet-ispolzovat-ii-dlya-kiberatak-na-ukrainu/ (last request: 12.10.2024) (In Russ)

15. *Plamenev I.* V FNS oprovergli vzlom nalogovoy sistemy ukrainskoy razvedkoy [Russian Federal Tax Service Denies Ukrainian Intelligence Hack of Tax System] / I. Plamenev [Electronic resource] // RBC: [website]. — URL: https://www.rbc.ru/society/12/12/2023/657890839a79477f74b0c200 (last request: 18.10.2024) (In Russ)

16. *Rudenko M.* Khakery vzlomali sayt Kiyevskogo oblsoveta [Hackers Hacked the Website of Kyiv Regional Council] / M. Rudenko [Electronic resource] // RIA Novosti: [website]. — URL: https://ria.ru/20231102/khakery-1907005140.html (last request: 15.10.2024) (In Russ)

17. Svetlana Tikhanovskaya ob'yavila "antivoennuyu mobilizatsiyu" [Svetlana Tikhanovskaya Announced "Anti-War Mobilization"] / [Electronic resource] // Euronews: [website]. — URL: https://ru.euronews.com/2022/03/02/belarus-tsikhanowskaya-antiwar-mobilisation (last request: 15.10.2024) (In Russ)

18. *Stepanova Y., Isakova T.* Utechki poluchili podkreplenie [Leaks Were Reinforced] / Y. Stepanova, T. Isakova [Electronic resource] // Kommersant: [website]. — URL: https://www.kommersant.ru/doc/5240325 (last request: 15.10.2024) (In Russ)

19. *Tairov R.* Byvshaya Group-IB zayavila o rekordnom roste kiberatak po politicheskim motivam [Former Group-IB Announced a Record Increase in Politically Motivated Cyber Attacks] / R. Tairov [Electronic resource] // Forbes: [website]. — URL: https://www.forbes.ru/tekhnologii/498860-byvsaa-group-ib-zaavila-o-rekordnom-roste-kiberatak-po-politiceskim-motivam (last request: 15.10.2024) (In Russ)

20. *Theise K., Schwartz Y.* Kak belorusskie "kiberpartizany" pomogayut Ukraine na voyne [How Belarusian "Cyber Partisans" Help Ukraine in the War] / K. Theise, Y. Schwartz [Electronic resource] // DW: [website]. — URL: https://www.dw.com/ru/belorusskie-kiberpartizany-pomogajut-ukraine-v-vojne-s-rossiej/a-62237250 (last request: 18.10.2024) (In Russ)

21. *Chikishev N.* Ukrainskaya razvedka zayavila o vzlome rossiyskoy nalogovoy. Vsya baza yakoby unichtozhena [Ukrainian Intelligence Claims to Have Hacked the Russian Tax Service. The Entire Database Allegedly Destroyed] / N. Chikishev [Electronic resource] // devby.io: [website]. — URL: https://devby.io/news/ukrainskaya-razvedka-zayavila-o-vzlome-rossiiskoi-nalogovoi-vsya-baza-yakoby-unichtozhena (last request: 15.10.2024) (In Russ)

22. *Antoniuk D.* Pro-Ukraine hackers claim to take down Russian internet provider / Daryna Antoniuk [Electronic Resource] // The Record from Recorded Future News: [site]. — URL: https://therecord.media/proukraine-hackers-claim-to-take-down-russian-isp (last request: 15.10.2024)

23. Check Point Research Team. The Russian-Ukrainian War, One Year Later / Check Point Research Team [Electronic Resource] // Check Point Blog: [site]. — URL: https://blog.checkpoint.com/2023/02/21/the-russian-ukrainian-war-one-year-later/ (last request: 18.10.2024)

24. 'Diya' personal data leak: Ukraine's Digital Transformation Ministry called out over social media manipulation and use of bots / [Electronic Resource] // https://mezha.net/: [site]. — URL: https://mezha.net/eng/bukvy/diya-personal-data-leak-ukraine-s-digital-transformation-ministry-called-out-over-social-media-manipulation-and-use-of-bots/ (last request: 15.10.2024)

25. *Gajos W.* How Russia's NoName057(16) could be a new model for hacking groups / Wiktoria Gajos [Electronic Resource] // CSO Online : [site]. — URL: https://www.csoonline.com/article/1270051/how-russias-noname05716-could-be-a-new-model-for-hacking-groups.html (last request: 12.10.2024)

26. *Huntley S.* Fog of war: how the Ukraine conflict transformed the cyber threat landscape / Shane Huntley [Electronic Resource] // Google Blog: [site]. — URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (last request: 15.10.2024)

27. Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective / [Electronic Resource] // FLASHPOINT: [site]. — URL: https://flashpoint.io/intelligence-101/killnet/ (last request: 18.10.2024)

28. *McLaughlin J.* Ukrainian hackers and intel officers partner up in apparent hack of a top Russian bank / Jenna McLaughlin [Electronic Resource] // NPR: [site]. — URL: https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (last request: 15.10.2024)

29. *McLaughlin J.* Ukrainian hacktivists fight back against Russia as cyber conflict deepens / Jenna McLaughlin [Electronic Resource] // NPR: [сайт]. — URL: https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war (last request: 15.10.2024)

30. *Pearson J.* Ukraine launches 'IT army,' takes aim at Russian cyberspace / James Pearson [Electronic Resource] // Reuters: [site]. — URL: https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/ (last request: 15.10.2024)

31. Render-Katolik A. The IT Army of Ukraine / Aiden Render-Katolik [Electronic Resource] // CSIS | Center for Strategic and International Studies: [site]. — URL: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine (last request: 18.10.2024)

32. *Sayegh E.* Turla Hacking Group: A Persistent International Threat / Emil Sayegh [Electronic Resource] // Forbes: [site]. — URL: https://www.forbes.com/sites/emilsayegh/2023/03/07/turla-hacking-group-a-persistent-international-threat/?sh=b888ef574980 (last request: 12.10.2024)

33. *Sayegh E.* APT28 Aka Fancy Bear: A Familiar Foe By Many Names / Emil Sayegh [Electronic Resource] // Forbes: [site]. — URL: https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/?sh=6349519059ad (last request: 15.10.2024)

34. *Sufi F.* Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges / Fahim Sufi [Electronic Resource] // MDPI: [site]. — URL: https://www.mdpi.com/2078-2489/14/9/485 (last request: 15.10.2024)

35. *Supruniuk I., Aushev Y.* CyberUnit.Tech & Cyber School: "Our mission is to elevate the perception of Ukraine as a country of innovation" / Iryna Supruniuk [Electronic Resource] // TechUkraine: [site]. — URL: https://techukraine.org/2022/06/30/yegor-aushev-cyberunit-tech/ (last request: 12.10.2024)

36. Srishti Singh Sisodia. Using fake profiles of women, Ukrainian hackers duped Russian soldiers to help military: Report / Srishti Singh Sisodia [Electronic Resource] // WION: [site]. — URL: https://www.wionews.com/world/using-fake-profiles-of-women-ukrainian-hackers-duped-russian-soldiers-to-help-military-report-513399 (last request: 15.10.2024)

Patrusheva Darya Andreevna – Senior Lecturer at the Department of History and Regional Studies, The Bonch-Bruevich Saint Petersburg State University of Telecommunications, (St. Petersburg, Russia), d.patrusheva@mail.ru

Ulasik Veronika Valeryevna – a third-year undergraduate student in Systems and Applied Programming of Information Systems, The Bonch-Bruevich Saint Petersburg State University of Telecommunications, (St. Petersburg, Russia), nika.ulasik@gmail.ru

Статья поступила в редакцию: 05.11.2024; принята к публикации: 21.12.2024

ДЛЯ ЦИТИРОВАНИЯ:

Патрушева Д. А., Уласик В. В. Хактивизм в контексте информационной войны: опыт российско-украинского конфликта (2022–2023) // Социогуманитарные коммуникации. – 2024. – № 4(10). – С. 118-127.

FOR CITATION:

Patrusheva D. A., Ulasik V. V. Haktivizm v kontekste informacionnoj vojny: opyt rossijsko-ukrainskogo konflikta (2022–2023) [Hacktivism in the context of information war: The experience of the russian-ukrainian conflict (2022–2023)] // Sociogumanitarnye kommunikacii [Social and humanitarian communications]. 2024. № 4(10). P. 118-127.