Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Т. Малярчук, Ю. Данык & Ч. Бриггс
Connections QJ 18, № 1-2 (2019): 110-129
https://doi.org/10.11610/Connections.rus.18.1-2.06

Рецензированная статья

Гибридная война и кибер воздействия на энергетическую инфраструктуру

***Тамара Малярчук,*[1] *Юрий Данык*[2] *и Чад Бриггс*[3]**

[1] *Житомирский государственный университет им. Ивана Франко, https://zu.edu.ua/en_index.html*

[2] *Национальный технический университет Украины «КПИ им. Игоря Сикорского», https://kpi.ua/en*

[3] *Университет Аляски, Анкоридж, США, https://www.uaa.alaska.edu/*

Резюме: Энергия – неотъемлемая часть всех отраслей экономики и социальной сферы, играющая особую роль в обеспечении безопасности развития современного общества. Поэтому энергетическая инфраструктура стала важнейшим компонентом гибридной войны. Деструктивный кибер шантаж в ней, как правило, сопровождается цепными и синергетическими эффектами, которые систематически оказывают влияние и охватывают все остальные сферы жизни общества и государства как в обычных, так и в особенно критических условиях. Авторы систематически и всесторонне проанализировали и представили в статье результаты исследований особенностей деструктивных кибер воздействий в национальной энергетике Украины и способов противодействия и защиты критической энергетической инфраструктуры.

Ключевые слова: гибридная война, энергетический комплекс, энергетическая инфраструктура, кибербезопасность, кибератака.

Введение

Дискуссии о гибридной войны часто концентрировались на дебатах об определениях точной природы термина и о том, охватывает ли термин «гибридная» то, что другие военные эксперты называют нелинейной войной,

войной полного спектра, войной четвертого поколения или другими подобными терминами. Точно так же при обсуждении киберконфликтов это явление рассматривалось как отдельная область, как если бы использование кибер-инструментов оставалось отличным от других форм конфликта. Гибридная война, которая *де-юре* ведется на территории Украины и *де-факто* охватывает большее количество участников со всего мира, по своему содержанию, формам и методам ведения может рассматриваться как специфический вариант четвертого поколения войны (4GW).

В гибридных конфликтах любой интенсивности боевые действия (операции) являются элементом других (несиловых) действий, взаимно скоординированных по единому плану, в основном экономического, политического, дипломатического, информационного, психологического, кибернетического, когнитивного и др. характера.[1] Это порождает дестабилизирующие внутренние и внешние процессы в государстве, являющемся объектом агрессии, такие как беспокойство и недовольство населения, миграция и акты гражданского неповиновения. Гибридные войны не объявляются и, следовательно, не могут быть завершены в классическом понимании окончания войн и военных конфликтов. Это своего рода перманентная война переменной интенсивности в нескольких секторах, с каскадными воздействиями и синергетическими деструктивными проявлениями, в которую в определенной степени сознательно или неосознанно вовлечено все население страны и международное сообщество. Воздействие ощущается во всех сферах жизни, во всех слоях общества и во всем государстве. Благодаря использованию инновационных технологий стало возможным переключить конфликт с преимущественно открытых и силовых (кинетических) средств на менее очевидные стратегии, ориентированные на структурную уязвимость противников, включая (что важно) достижение когнитивного преимущества над ними.

Применительно к событиям на Украине с 2013 года основное внимание часто уделялось вторжению России в Крым в 2014 году и последующему содействию поддерживаемым Россией анклавов в восточных украинских регионах Донбасса и Луганска. Эти операции – от появления так называемых «зеленых человечков» в Симферополе до крушения рейса № 17 Малазийских авиалиний несколькими месяцами позже – сфокусированы на довольно обычных (хотя и нерегулярных) формах конфликта. Часто упускаются из виду более широкие стратегические цели противника при проведении кампании гибридной войны и широкий спектр инструментов, используемых для достижения этих целей.

Как считают многие авторы, гибридная война – явление не новое, поскольку она представляет собой скоординированные действия как государственных, так и негосударственных субъектов по проведению кампании

[1] Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, “Hybrid War: High-tech, Information and Cyber Conflicts,” *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

действий, которые варьируют от информационной войны до прямого кинетического конфликта.[2] Стратегия Российской Федерации в отношении Украины после Майдана в основном направлена на дестабилизацию и делегитимацию правительства, что является частью усилий по предотвращению интеграции Украины с западноевропейскими институтами и предотвращению эффективного вмешательства со стороны западных стран или стран НАТО. Хотя оккупация Крыма и продолжающийся конфликт на востоке Украины служат этой цели, был предпринят более широкий, но менее заметный набор действий, направленных на эрозию устойчивости украинских институтов. Вместо того, чтобы сосредотачиваться на самой гибридной войне или киберсфере как отдельного домена враждебных действий, цель этой статьи – проиллюстрировать и объяснить использование кибероружия против энергетической инфраструктуры.

Опять же, хотя это и не новая стратегия, осуществляемая повстанцами или кампаниями стратегических бомбардировок, нацеливание на энергетическую инфраструктуру является эффективным способом повышения уязвимости государства или общества, одновременно давая сигнал другим потенциальным противникам об их собственной уязвимости и возможностях наносить ущерб крупным отраслям их экономики. Кибер-инструменты обеспечивают асимметричное преимущество без учета географического расстояния, а это означает, что небольшие группы могут наносить широкомасштабный ущерб, избегая при этом обычной атрибуции и правил сдерживания.[3] Во время Холодной войны Соединенные Штаты проводили гибридные операции в таких странах, как Филиппины в начале 1950-х годов и Вьетнаме в 1960-х годах, используя целый ряд методов – от создания газет и радиостанций до поддержки повстанцев и наемников и активного участия боевых частей США. Опыт США может быть поучительным, поскольку он иллюстрирует две очень разные стратегические цели при использовании гибридных методов – либо попытки стабилизировать, либо дестабилизировать иностранный режим. В то время как в некоторых случаях, например на Филиппинах, усилия по стабилизации были в значительной степени успешными, в ряде примеров от Вьетнама до Афганистана, США добились гораздо меньшего успеха в своих усилиях по стабилизации. С другой стороны, дестабилизация, по-видимому, является более успешным применением методов

[2] Robert Wilkie, “Hybrid Warfare: Something Old, Not Something New,” *Air and Space Power Journal* 23, no. 4 (Winter 2009): 13-18; NicuPopescu, “Hybrid Tactics: Neither New Nor Only Russian,” *EUISS Issue Alert* 4 (European Union Institute for Security Studies, January 2015), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

[3] Dinos Kerigan-Kyrou, “Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges,” *Connections: The Quarterly Journal* 12, no. 3 (Summer 2013): 109–17, http://dx.doi.org/10.11610/Connections.12.3.06.

гибридной войны, как, например, в контролируемых США действиях в Центральной Америке и Чили, или в Иране в 1953 году.[4]

Для целей этой и последующих статей гибридная война определяется как полное использование государственных и негосударственных инструментов для изменения стабильности и легитимности ключевых систем и институтов в данном регионе. Обратите внимание, что теоретически это означает, что методы гибридной войны могут использоваться в законных целях, а также для дестабилизации, и это часто делается при атаке противника и одновременной поддержке своего государства и союзников / прокси-субъектов. В то время как двойное использование гибридных инструментов не так очевидно в энергетическом секторе, эта статья является одной из серии, в которой также исследуется социальная устойчивость и роль иностранного вмешательства (например, отношения Европейского Союза с Украиной), где играть несколько ролей становится все более важным, и где кибер-методы затрудняют отслеживание этих усилий. Энергетическая инфраструктура и кибератаки – удачное место для начала исследования из-за существующей истории атак и сходства между государствами в их потребности защищать источники энергии и их уязвимости для кибер-инструментов.

Такими возможностями располагает не только Россия. Червь Stuxnet (приписываемый, возможно, Израилю и США) эффективно наносил физический ущерб центрифугам с ядерным топливом, не подключенным к какой-либо внешней сети и рассматриваемым иранцами как безопасные в отношение внешнего вмешательства или нападения. Stuxnet был элегантной программой, которая могла легко перемещаться без обнаружения с компьютера на компьютер, не причиняя вреда и не вмешиваясь в работу какой-либо системы, пока, наконец, не нашла свой путь к конкретным центрифугам с компьютерным управлением в Иране. Оказавшись там, червь вносил небольшие изменения в работу высокоскоростных машин, сдвигая калибровку ровно настолько, чтобы повредить или уничтожить их, не вызывая подозрений, что происходит внешняя атака.[5] Точно так же Китай и даже более мелкие государства, такие как Северная Корея, обладают антиэнергетическим кибер-потенциалом, а заметный потенциал кибератак против энергетики также продемонстрировали такие негосударственные субъекты, как Аль-Каида и ИГИЛ.[6]

---

[4] Max Boot, *The Road Not Taken: Edward Lansdale and the American Tragedy in Vietnam* (New York: Liveright Publishing, 2018).

[5] Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy* 9, no. 3 (May-June 2011): 49-51.

[6] Lukáš Tichý and Jan Eichler, "Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State," *Studies in Conflict & Terrorism*, 41:6 (2018): 450-473, https://doi.org/10.1080/1057610X.2017.1323469.

Концепция устойчивости

Как писали Конклин и Конке, большая часть кибербезопасности была построена вокруг концепции «ограждения» компьютерных систем от внешних злоумышленников и вокруг защиты данных, а не на сосредоточении внимания на устойчивости системы в целом. Их предложение состояло в том, чтобы сосредоточить внимание в большей степени на функциональности, а не на отдельных атаках, подход, который уже существует в энергетическом секторе, но который указывает на несоответствие между энергетической безопасностью и уязвимостями, присутствующими в инфраструктуре из связанных с кибер-системами систем.[7] Таким образом, энергетическая безопасность в отношение кибератак опирается на более широкую концепцию устойчивости, которая связана не только с фактическим производством и передачей энергии, но и с теми системами, которые энергетика поддерживает и узаконивает. Если общество лишается энергии, особенно сильно индустриальное и технологически зависимое, тогда пресловутая коверная дорожка выдергивается из-под ног всех систем обеспечения.

Сети устойчивости могут быть смоделированы в соответствии с типом и схемой соединений (топологией) между различными частями системы, будь то отдельные лица, электрические соединения или экологические отношения. Поскольку сетевые соединения являются функциональными, они редко бывают случайными, а наоборот, сосредоточены на критических узлах, которые обеспечивают важные связи внутри системы. В экологических науках эти критические узлы часто называют «ключевыми видами», которые, даже если они не являются наиболее заметными представителями экосистемы, имеют решающее значение для ее эффективного функционирования. В социальных системах такими критическим узлами могут быть ключевые люди или центры активности сообщества, которые обеспечивают связь между людьми, которые в противном случае не могут взаимодействовать. А в отношение Интернета критическими узлами являются либо наиболее заметные центры активности, такие как Google, либо могут быть представлены в виде ключевых серверов или линий связи. Однако во всех вышеперечисленных случаях эти сети часто называют «безмасштабными», что означает, что они имеют тенденцию быть устойчивыми, поскольку случайные отказы в любой части системы могут быть компенсированы.[8]

Энергетические сети часто конфигурируются по-другому, поскольку вместо того, чтобы быть устойчивыми и позволять перенаправлять мощность в

---

[7] William Arthur Conklin and Anne Kohnke, “Cyber Resilience: An Essential New Paradigm for Ensuring National Survival,” in *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018*, National Defence University, Washington D.C., USA, 8-9 March 2018, ed. Dr. John S. Hurley and Dr. Jim Q. Chen (Reading, UK: Academic Conferences and Publishing International Limited, 2018), p. 126.

[8] Sarah Dunn and Sean Wilkinson, “Hazard Tolerance of Spatially Distributed Complex Networks,” *Reliability Engineering & System Safety* 157 (2017): 1-12.

случае сбоя, традиционная энергетическая инфраструктура была построена на централизованных узлах. Образец энергетической инфраструктуры двадцатого века представлял собой крупная электростанция (на ископаемом или ядерном топливе), которая затем передает электроэнергию в населенные пункты с соответствующими подсетями электрических трансформаторов.[9] Большая часть работы по повышению устойчивости энергетических систем была направлена на предотвращении каскадных отказов в электрических сетях, где отказ нескольких критических узлов приводит к отключению электроэнергии в больших географических районах, что неоднократно наблюдалось в Северной Америке. Это была форма устойчивости, но в сочетании с элементами хрупкости, что означало, что система была хрупкой и ее можно было легко сломать с помощью достаточной внешней силы. Пуэрто-Рико после урагана Мария в 2017 году является ярким примером.[10] Гражданская устойчивость в энергетическом секторе в меньшей степени сосредоточена на самих электростанциях, хотя экологические факторы все чаще нарушают способность крупных электростанций противостоять наводнениям и другим экологическим опасностям. Хотя наиболее ярким примером была катастрофа на Фукусиме в 2011 году, энергетические сооружения в Северной Америке и Европе становятся все более уязвимыми.[11]

Социальные, политические и энергетические сети не работают независимо, а «вложены» друг в друга. Высокоустойчивые социальные и политические связи основаны на деятельностях, которые не могут осуществляться долго без более фундаментальных энергетических и экологических сетей. Это делает уязвимыми даже самые прочные социальные сети в случае нарушения энергоснабжения. Как основная потребность, коммунальные услуги, такие как поставка энергии, поставка воды и канализация, дают отражение на легитимность управляющих властей, и доверие к этим учреждениям быстро ослабевает, когда основные услуги не могут быть удовлетворены. В Косово, например, несмотря на высокое общественное доверие к безопасности, обеспечиваемой НАТО/ KFOR в стране, электроэнергетические компании KEK и KEDS подвергались публичной критике и недоверию, и несмотря на приватизацию, все же негативно и серьезно повлияли на общественное восприятие легитимности правительства и доверия к его способ-

---

[9] Dong Hwan Kim, Daniel A. Eisenberg, Yeong Han Chun, and Jeryang Park, "Network Topology and Resilience Analysis of South Korean Power Grid," *Physica A: Statistical Mechanics and Its Applications* 465 (January 2017): 13-24, https://doi.org/10.1016/j.physa.2016.08.002.

[10] Maria Gallucci, "Rebuilding Puerto Rico's Grid," *IEEE Spectrum* 55, no. 5 (May 2018): 30-38, https://doi.org/10.1109/MSPEC.2018.8352572.

[11] Cleo Varianou Mikellidou, Louisa Marie Shakou, Georgios Boustras, and Christos Dimopoulos, "Energy Critical Infrastructures at Risk from Climate Change: A State of the Art Review," *Safety Science* 110, Part C (December 2018): 110-120, https://doi.org/10.1016/j.ssci.2017.12.022.

ности обеспечивать безопасность.[12] В Ираке вооруженные силы США провели исследование, которое выявило сильную связь с поддержкой повстанцев в тех районах Багдада (особенно в Садр-Сити), где повстанцы перекрыли доступ к воде, электричеству и канализации.[13] Разжигание нестабильности с помощью базовых услуг может быть эффективным и надежным способом подорвать устойчивость общества и сделать его более уязвимым. Для таких стран, как Украина, с ее травматическим опытом чернобыльской катастрофы 1986 года, связь между энергетической безопасностью и легитимностью правительства может быть еще более хрупкой.

Атаки и уязвимости в Украине

Современное общество практически полностью зависит от состояния защищенности информации и кибер-инфраструктуры во всех сферах жизнедеятельности человека. Возможность использовать как информационные, так и кибертехнологии, а также информационно-коммуникационные сети для достижения своих целей имеют не только государственные структуры стран, но и криминальные и террористические организации. В связи с этим обеспечение кибер и информационной безопасности критически важной инфраструктуры государства стало решающим условием для обеспечения обороноспособности государства и его экономического и социального развития. В январе 2018 года Сенат США выпустил доклад,[14] в котором отмечалось, что с 2014 года Россия неустанно и по разному использует киберпространство Украины в качестве кибер театра и полигона для испытания кибероружия. Во многих случаях кибератаки были нацелены на украинскую систему распределения электроэнергии, в результате чего на долгое время выводились из строя секторы экономики, инфраструктуры и жилья. После атаки России на украинскую энергосистему американские представители Министерства энергетики, Министерства внутренней безопасности, ФБР и Североамериканской корпорации по надежности электроснабжения увеличили свое участие в работе по электроснабжению. Признавая необходимость изучения этих кибер-воздействий, они работали вместе, чтобы понять тактику и практику российского правительства, спрогнозировать типы буду-

[12] Mentor Vrajolli, *Kosovo Security Barometer,* Seventh Edition (Pristina: Kosovar Centre for Security Studies, 1 February 2018), http://www.qkss.org/en/Reports/Kosovo-Security-Barometer-Seventh-Edition-1050.

[13] David E. Mosher, Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen, and Henry H. Willis, *Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict* (Santa Monica, CA: Rand Corporation, 2008), 90-91.

[14] "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (U.S. Government Publishing Office, January 10, 2018), https://www.hsdl.org/?view&did=806949.

щих кибератак и разработать эффективные меры защиты от них. Сотрудничество с Украиной в противодействии этим угрозам, опять же, считается важнейшим элементом киберзащиты США.

Глубокое проникновение энергетики во все отрасли экономики и в социальную сферу определяет ее особую роль в обеспечении безопасности современного развития общества. Энергетическая безопасность характеризует степень выполнения энергетическим комплексом его функций в обществе и государстве в обычных, критических и чрезвычайных обстоятельствах.[15] Предприятия и учреждения энергетического сектора играют ведущую роль в развитии государства.[16] Промышленность остается основным потребителем электроэнергии, хотя ее доля в общем потреблении электроэнергии в мире снижается. В промышленности электроэнергия используется для приведения в действие различных механизмов и технологических процессов. На сегодняшний день коэффициент электрификации силового привода в промышленности составляет 80 %. При этом около 1/3 электроэнергии тратится непосредственно на технологические нужды.[17] Объекты энергетического сектора являются стратегически важными и должны непрерывно функционировать и обеспечивать предоставление качественных услуг.[18]

На территории Украины в каждом регионе есть энергетические системы, которые относятся к критической инфраструктуре. Каждая из них обладает так называемыми «критическими узлами», нарушение работы которых приводит к нарушению функциональности сети и потенциально вызывает каскадные отказы в сетях. Схематично этот комплекс представлен в таблице 1.

Все структурные элементы энергетики относятся к определенной иерархии, системе контроля и системе безопасности. Основой электроэнергетики является единая энергосистема Украины, которая централизует поставки электроэнергии внутренним потребителям, а также ее экспорт и импорт. Система объединяет восемь региональных энергосистем (Днепровская, Донбасса, Западная, Крымская, Южная, Юго-Западная, Северная, Центральная), соединенных между собой системообразующими и межгосударственными высоковольтными линиями электропередачи. По данным Государственного комитета статистики Украины, наибольшая доля электроэнергии вырабатывается на тепловых электростанциях (около 50 %), на атомных станциях (45 %) и на гидроэлектростанциях (5 %).

---

[15] Концепция развития сектора безопасности и обороны Украины, введенная в действие Указом Президента Украины от 14 марта 2016 г. № 92/2016.

[16] Стратегия кибербезопасности Украины, утвержденная Указом Президента Украины от 15 марта 2016 г. № 96 (Officer Vision of Ukraine, 2016), # 23.

[17] Закон Украины «Основные принципы кибербезопасности Украины» № 2163-VIII от 5 октября 2017 года, http://zakon.rada.gov.ua/laws/show/2163-19.

[18] Стратегия национальной безопасности Украины, утвержденная Указом Президента Украины от 26 мая 2015 г. № 287/2015 г., http://zakon.rada.gov.ua/287/2015.

Таблица 1. Энергетический комплекс Украины.

<table>
<tr><th colspan="2">Топливная промышленность</th><th colspan="4">Электроэнергетика</th><th>Инфраструктура генерации</th></tr>
<tr><td colspan="2">1. Угольная промышленность</td><td colspan="4">1.Тепловые электростанции</td><td>1. Транспорт</td></tr>
<tr><td colspan="2">2. Газовая промышленность</td><td colspan="2">Государственная региональная электростанция</td><td colspan="2">Теплоэлектроцентраль</td><td>a) Трубопроводный</td></tr>
<tr><td colspan="2">3. Нефтяная промышленность</td><td colspan="4">2. Гидроэлектростанции</td><td>b) Железнодорожный</td></tr>
<tr><td>a) Добыча нефти</td><td>b) Нефтепереработка</td><td colspan="2">Гидро-электростанции</td><td colspan="2">Гидроаккумулирующие электростанции</td><td>c) Водный</td></tr>
<tr><td colspan="2" rowspan="2">4. Торфяная промышленность</td><td colspan="4" rowspan="2">3. Атомные электростанции</td><td>d) Автомобильный</td></tr>
<tr><td>e) Воздушный</td></tr>
<tr><td colspan="2" rowspan="3">5. Сланцевая промышленность

6. Химическая промышленность</td><td colspan="4">4. Альтернативные источники энергии</td><td>2. Линии электро-передач</td></tr>
<tr><td>a) Ветряные электростанции</td><td>b) Солнечные электро-станции</td><td>c) 3D альтернативные ПЭЯ</td><td>d) Биотопливные электростанции</td><td rowspan="2">3. Водоснабжение
a) Система управления;
4. Система поддержки персонала</td></tr>
<tr><td colspan="2">e) Топливные электростанции</td><td colspan="2">f) Геотермальные станции</td></tr>
</table>

Угрозы в энергетическом секторе

Весь набор угроз, которые могут повлиять на функционирование энергосистем, можно условно разделить на обычные угрозы (вероятные сбои и аварии) и чрезвычайные угрозы (они уникальны по происхождению, характеру развития и последствиям). Различные формы резервирования мощностей, разработки и транспортировки топливно-энергетических ресурсов, системы гарантированного энергоснабжения, создание резервов топливно-энергетических ресурсов служат для противодействия обычным угрозам в энергосистемах. Обыденные явления практически исключают создание угрозы энергетической безопасности в условиях развития и функционирования национальной экономики. Напротив, необычные воздействия могут негативно повлиять на энергетический комплекс в целом. Среди чрезвычайных угроз ведущую роль играют киберугрозы. Киберугрозы способны спровоцировать такие проблемы, как нарушение обеспечения энергоресурсами и

чрезвычайные ситуации в энергетическом комплексе государства. Они реализуются в виде разнообразных деструктивных кибер-воздействий.

Разрушительные кибер воздействия могут вызывать:

- Целенаправленные атаки (повышенная постоянная угроза);
- Воздействия на системы управления;
- Воздействия через социальные сети;
- Атаки на банковские системы (кража денег);
- Аппаратные ошибки (инструментальные ошибки) в микросхемах и прошивках компьютерного и сетевого оборудования.

Такие киберугрозы могут быть реализованы путем воздействия как на весь энергетический комплекс в целом, так и на его элементы в отдельности, а также путем достижения синергии результатов. Воздействие может осуществляться комплексно, одновременно, последовательно или смешанно на автоматизированные системы управления, на персонал, на финансовую систему энергетики, на программно-аппаратный комплекс. Самым уязвимым местом в единой энергосистеме являются автоматизированные системы управления.

Анализ кибер воздействий на объекты критической инфраструктуры энергетики в 2014-2018 гг.

Проблема кибербезопасности государственного энергетического сектора имеет решающее значение для национальной безопасности и национальной обороны, а также для экономического и социального развития.

В 2014–2018 годах были осуществлены хорошо спланированные синхронизированные кибератаки на элементы энергетического комплекса Украины. На какое-то время нарушителям удалось управлять комплексом, а в некоторых случаях даже нарушать функционирование как системы управления, так и нормальное функционирование элементов энергокомплексов. Целями этих атак, возможно, были проверка надежности системы кибербезопасности этой критически важной инфраструктуры, установление особенностей функций системы кибербезопасности энергетических компаний и их реакции на различные кибер воздействия и инциденты. Было показано, что чрезмерно сложный контроль над информационными системами может сделать комплексные энергетические объекты уязвимыми для кибератак. Наиболее опасными кибер-воздействиями на объекты энергетического комплекса являются те, которые вызывают или сопровождаются цепными деструктивными воздействиями непосредственно на энергетический объект, который затем подключается к другим объектам инфраструктуры и сферам повседневной жизни нации.

Еще одной особенностью кибератак на объекты энергетического комплекса Украины было начальное рассредоточение с конечной направленностью на определенные систематические многоспектральные результаты и разноплановые последствия.

В ходе анализа кибератак выяснилось, что атаки не были одиночными, а проводились синхронно. Все они оказывали разрушительное воздействие на АСУ энергетических объектов. Основной синхронный деструктивный киберэффект был сосредоточен на уязвимых элементах автоматизированных систем управления. Перед основной кибератакой осуществлялась предварительная кибератака на сервисно-диспетчерскую систему с целью отказа в обслуживании потребителей. Применение нескольких деструктивных концентрированных кибератак на энергокомплекс осуществлялось в рамках масштабной кибероперации, направленной на нарушение одновременно нескольких объектов энергокомплекса Украины.

Группы, ответственные за многие украинские кибератаки, Telebots, BlackEnergy и Gray Energy, были более тесно или более слабо связаны с российскими государственными спецслужбами, подобными британской GCHQ.[19] Однако отсутствие прямой атрибуции не умаляет значение стратегического использования таких инструментов для дестабилизации и делегитимации украинского государства. Напротив, такие замаскированные подходы к конфликту являются яркими примерами того, как кибер-инструменты могут быть использованы в современных концепциях гибридной войны, когда уязвимости критически важной инфраструктуры подвергаются атакам, чтобы ослабить государственную поддержку и функционирование и усилить недоверие потенциальных внешних партнеров. Второстепенная цель кибератак на энергетическую инфраструктуру может заключаться в том, чтобы дать сигнал другим (например, Великобритании, США, Германии) об их уязвимостях, причем украинские атаки служат подтверждением концепции. В любом случае действия кибер-атакующих сильно скоординированы, их трудно отследить и атрибутировать, и они представляют собой крайне асимметричные некинетические атаки. Эти атаки являются новыми техническими областями конфликта, особенно в тех случаях, когда целью является непрекращающееся состояние нестабильности, а не традиционная концепция «полной победы» на поле боя.

Одной из важных составляющих энергосистемы Украины является система управления. Система управления энергосистемой играет ведущую роль в функционировании всего энергетического комплекса Украины. На автоматизированную систему управления может быть оказано мощное кибер воздействие, которое может привести к нарушению управления отдельными объектами энергетики или энергетическим комплексом в целом. Автоматизированная система управления энергосистемой должна быть устойчивой к кибер-воздействиям и иметь соответствующую комплексную систему противодействия кибератакам.

[19] Jack Stubbs, “Hackers Accused of Ties to Russia Hit Three East European Companies: Cybersecurity Firm,” *Reuters*, October 17, 2018, https://uk.reuters.com/article/us-russia-cyber/hackers-accused-of-ties-to-russia-hit-three-east-european-companies-cybersecurity-firm-idUKKCN1MR1BO.

В декабре 2015 года была зафиксирована повышенная постоянная угроза (APT) в автоматизированной системе управления энергосистемой. Атаке подверглись внутренние сети украинской энергокомпании Прикарпатьеоблэнерго (ПАО).[20] В результате этой кибератаки значительная часть области и областной центр остались без электроснабжения в течение нескольких часов. Было остановлено 30 подстанций. Около 230 тысяч человек лишились энергоснабжения на срок от одного до шести часов. В ходе атаки использовалось вредоносное ПО BlackEnergy.[21] Группа BlackEnergy начала атаку на украинскую электросеть с помощью семейств ПО BlackEnergy и KillDisk. Это было последнее известное использование вредоносного ПО BlackEnergy в реальном мире. После атаки выяснилось, что группа BlackEnergy состоит как минимум из двух подгрупп: TeleBots и GrayEnergy.

Основная цель группы TeleBots – осуществление кибератак с целью проведения диверсий в Украине, что достигается за счет атак на компьютерные сети (CNA). Эта группа совершила множество разрушительных атак, в том числе:

- серия атак в декабре 2016 года с использованием обновленной версии того же вредоносного ПО KillDisk, разработанного для операционных систем Windows и Linux;
- известная атака Petya / NotPetya в июне 2017 года с использованием бэкдоров, встроенных в украинскую бухгалтерскую программу MEDOC;
- атака с использованием семейства ПО BadRabbit в октябре 2017 г.

Специалисты ESET в течение нескольких лет отслеживали деятельность группы GreyEnergy. Группа GreyEnergy использует уникальное семейство вредоносных программ. Дизайн и архитектура этого вредоносного ПО очень похожи на уже известное семейство BlackEnergy. Помимо концептуального сходства вредоносного ПО, ссылки указывают на то, что группа, стоящая за вредоносным ПО GreyEnergy, тесно сотрудничает с группой TeleBots. В частности, в декабре 2016 года команда GreyEnergy разработала червя, похожего на NotPetya, а позже еще более продвинутая версия этой вредоносной программы использовалась группой TeleBots во время атаки в июне 2017 года. GreyEnergy имеет более широкие цели, чем группа TeleBots. GreyEnergy в первую очередь интересуется промышленными сетями различных организаций, отвечающие за критическую инфраструктуру, и, в отличие от TeleBots, группа GreyEnergy не ограничивается только Украиной.

В конце 2015 года специалисты ESET впервые обнаружили вредоносное ПО GreyEnergy, нацеленное на энергетическую компанию в Польше. Но

---

[20] Kim Zetter, “Russia’s Hacking Attack on the Ukrainian Power System: How It Was,” *Texty.org.ua*, http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak.

[21] Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present* (New York: Auerbach Publications, 2017).

позже, как и в случае с BlackEnergy и TeleBots, фокус группы GreyEnergy сместился на Украину. Злоумышленники сначала проявляли интерес к энергетическому сектору, а затем к транспортной инфраструктуре и другим важным объектам. О последнем использовании вредоносного ПО GreyEnergy было сообщено в середине 2018 года.

Вредоносное ПО GreyEnergy является модульным, и в отличие от Industroyer, специалисты ESET не обнаружили никаких модулей, управляемых ПСУ, а это означает, что оно нацелено именно на промышленные системы управления, но такая система может быть объектом воздействия с использованием и других методов. По крайней мере, операторами был обнаружен один случай использования этого вредоносного ПО. Модуль может стереть диск, чтобы нарушить бизнес-процессы в компании и скрыть следы.[22] Одна из наиболее ярких деталей, выявленных в ходе исследования ESET, заключается в том, что один из обнаруженных образцов GreyEnergy был подписан действующим цифровым сертификатом, который, вероятно, был украден у тайваньской компании, производящей оборудование для ПСУ. Другими словами, группа GreyEnergy буквально следовала методам разработки Stuxnet.

Кроме того, синхронные атаки были осуществлены на энергокомпании «Черновцыоблэнерго» и «Киевоблэнерго», но с меньшими последствиями. 23 декабря 2015 года несанкционированная группа лиц вмешалась в работу информационно-технологической системы удаленного доступа к телеуправлению оборудованием подстанций 35-110 кВ ПАО «Киевоблэнерго». С 15:31 до 16:30 по местному времени было полностью или частично отключено пятнадцать городов и сел в Мироновском, Макаровском, Белоцерковском, Фастовском, Сквирском, Рокитнянском, Кагарлыкском, Иванковском и Яготинском административных округах. Более 80 000 потребителей остались без электричества. В результате атаки произошли сбои в системе удаленного доступа. Отключено было 30 станций, снабжающих несколько стратегических объектов области: предприятия, учреждения, организации, население. Электричество восстановили 23 декабря 2015 года в 18:56.[23]

Система управления была уязвима для подобных кибератак. Ответ на кибератаку был несвоевременным, а система безопасности не справилась со своими функциями. С помощью вредоносного ПО злоумышленник может контролировать и в некоторых приложениях управлять частью или всей автоматизированной системой управления. Последствия такой атаки могли быть использованы для проверки работы системы безопасности и системы реагирования энергетической компании на критическую ситуацию.

---

[22] "GreyEnergy: A Successor to BlackEnergy," White Paper (GreyEnergy, October 2018), www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.

[23] «Крупнейшие кибератаки на Украину с 2014 года», *Новое время*, 24, 7 июля 2017, https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

В целом кибератака была комплексной и в определенной степени систематически организована через:

- Предварительное заражение сетей с помощью поддельных писем;
- Получение контроля над автоматизированной системой управления путем отключения операций на подстанциях;
- Отказ элементов АСУ;
- Удаление информации на серверах и рабочих станциях (утилита Kill Disk);
- Атак на телефонную сеть колл-центров с целью отключения обслуживания текущих абонентов.

В период с 19 по 20 января 2016 года была проведена кибератака с помощью кибер-инструмента Joint Conflict and Tactical Simulation Enhancements, которая также была направлена на нарушение работы системы управления путем установки вредоносного ПО, присланного электронной почтой.[24] Другая кибератака, проведенная в ночь с 17 на 18 декабря 2016 г., была менее масштабной. Произошел срыв работы подстанции «Северная» энергокомпании «Укрэнерго». Потребители в северной части Киева и прилегающих районах остались без электричества. Нападавшие не причинили значительного ущерба; целью нападения была «демонстрация силы». Как и в предыдущих случаях, это нападение было частью операции против государственных учреждений Украины.[25]

Основные особенности продвинутых постоянных угроз (Advanced Persistent Threats) заключаются в том, что они, как правило:

- нацелены на элементы критической инфраструктуры
- проводятся группой высококвалифицированных хакеров
- тщательно маскируются с помощью специально разработанных программных средств (например, специальных Shell-кодов, Root Kitta)
- долгое время остаются неизвестными
- сопровождаются разведывательными или деструктивными действиями
- и являются элементами разведывательных и диверсионных операций.

Анализ кибер воздействий представлен в таблице 2.

---

[24] "Zillya! Antivirus Has Analyzed the Cyber Attacks on Infrastructure Objects in Ukraine," February 17, 2016, Antivirus Zillya, Certificated for use by public and state authorities, https://zillya.ua/zillya-antivirus-provela-analiz-kiberatak-na-infrastrukturni-ob-kti-ukra-ni.

[25] Vitaliy Tchervonenko, "Was There an Attack on the Regional Power Company," BBC Ukraine, January 6, 2016, https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc.

Таблица 2. Анализ кибер атак.

Объект воздействия	Использованные инструменты	Способ проникновения	Воздействие	Последствия
2015				
«Прикарпатье Облэнерго»	DoS-атака на коллцентры «Облэнерго» методом «отказа в обслуживании»[26]	Сеть Интернет	Насыщение сетевого оборудования большим количеством внешних запросов	Потребители не могли сообщать об отключении электроэнергии
	Расширенная постоянная угроза (Advanced Persistent Threat)	Сеть SCADA, установка вредоносного ПО «BlackEnergy»	Перехват управления системы в сети SCADA через украденные аккаунты; отправка команд на отключение систем бесперебойного питания, которые уже были реконфигурированы. После этого отключение систем безопасности, приводящее к прерыванию подачи электроэнергии	Отключено около 30 подстанций, около 230 тыс. человек остались без электричества от одного до шести часов.
«Черновцы облэнерго»	DoS-атака на коллцентры «Облэнерго» методом «отказа в обслуживании»	Сеть Интернет	Насыщение сетевого оборудования большим количеством внешних запросов	Потребители не могли сообщать об отключении электро-энергии
	Утилита Kill Disk	Сеть Интернет	Уничтожение информации на серверах и рабочих станциях	Отказ элементов ИТ-инфраструктуры
	APT-атака, обнаружение вредоносного ПО «BlackEnergy»	Сеть SCADA	Захват управления автоматизированными диспетчерскими систем с проведением остановок на подстанциях	Перерыв в подаче электроэнергии составил от 1 до 3,5 часов. Всего недодано 73 МВтч

[26] Государственная энергетическая компания Украины.

				(0,015% суточного потребления Украины)
«Киевское облэнерго»	Расширенная постоянная угроза (APT)	Система удаленного доступа	Несанкционированное вмешательство в АСУ	Более 80 378 потребителей без электричества. Отключено электроснабжение 30 узловых подстанций, питающих ряд стратегических объектов, более 80 тыс. потребителей остались без электричества в течение одного-трех часов.
2016 год				
«Киевское облэнерго»	Вредоносное ПО Crash Override (атака была полностью автоматизирована)	Сеть Интернет	Перехват управления энергосистемой, автоматическая разгрузка подстанций	Подстанция «Пивничная» с питанием для собственных нужд от подстанции полностью отключена. Снижение нагрузки на 144,9 МВт ПАО «Киевэнерго» и 58 МВт ОАО «Киев-облэнерго». Киевская АЭС тоже была отключена от системы с потерей мощности для собственных нужд.

Основные кибератаки различаются по своим последствиям и способам действия. Атаки на энергокомпании в 2015 году не были полностью самоорганизованными. В 2016 году вредоносные программы, которые уже предусматривали самоорганизацию действий в процессе атак и работы, стали более работоспособными. Также, проведя исследование специалисты компании ESET, констатировали, что «Crash Override» способен физически разрушать энергосистемы. Программное обеспечение CrashOverride [27] имеет возможность отправлять команды в электросеть на включение или отключение питания. По их данным, Crash Override может использовать известную уязвимость оборудования Siemens, в частности цифрового реле Siprotec. Такие реле устанавливаются для защиты и управления распределительными и передающими электросетями. Майк Ассанте из американской компании по кибербезопасности SANS Institute установил, что отключение цифрового реле может привести к тепловой перегрузке электросети. Это очень серьезная угроза для трансформаторов и любого оборудования, находящегося под напряжением. Таким образом, Crash Override может обеспечить спланированную атаку на несколько «критических узлов» энергетического комплекса. Тогда есть вероятность отключения электроэнергии во всем государстве, поскольку нагрузка перемещается из одного региона в другой.

Автоматизированные энергосистемы энергетических комплексов уязвимы для кибератак. В результате нашего анализа кибератак мы можем выделить следующие категории возможных кибератак:

- Направленные на целевые компоненты: электронные вычислительные устройства, такие как удаленные терминалы (RTU) или человеко-машинный интерфейс (HMI),[28] обычно имеют интерфейс для удаленной настройки или управления. С помощью удаленного доступа злоумышленник может перехватить управление устройством и вызвать сбои, например, внести изменения в данные, передаваемые оператору, повредить оборудование или вызвать полный или частичный отказ устройства.
- Ориентированные на протоколы: почти все современные протоколы передачи данных хорошо документированы, а их описание открыто. Например, стандарт DNP3 распространен в системах управления энергопотреблением в Северной Америке.[29] Его спецификация доступна

[27] Middleton, *A History of Cyber Security Attacks*.

[28] Muhammad Baqer Mollah and Sikder Sunbeam Islam, “Towards IEEE 802.22 Based SCADA System for Future Distributed System,” in *Proceedings of 2012 International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, Bangladesh, 18-19 May 2012, https://doi.org/10.1109/ICIEV.2012.6317474.

[29] Salman Mohagheghi, Mirrasoul Mousavi, J. Stoupis, and Z. Wang, “Modeling Distribution Automation System Components Using IEC 61850,” in *Proceedings of the 2009 IEEE Power & Energy Society General Meeting*, Calgary, AB, Canada, July 26-30, 2009, https://doi.org/10.1109/PES.2009.5275841.

каждому по невысокой цене. Злоумышленник может внести изменения в эту информацию, что может привести к значительным финансовым затратам из-за перепроизводства электроэнергии, включения ЛЭП во время работы на них, повреждения оборудования, перегрузки системы.

27 июня 2017 года на украинские учреждения и организации была совершена масштабная деструктивная хакерская атака («Petya»). Атаке подверглись непосредственно и «критические узлы» энергетики (Укрэнерго, Киевоблэнерго, Днепроэнерго, Запорожьеоблэнерго, Чернобыльская АЭС). Эта кибератака была направлена на нарушение работы веб-сайтов компаний и систем поддержки клиентов. Ущерб информационным системам украинских компаний произошел из-за обновления программного обеспечения, предназначенного для отчетности и документооборота M.E.Doc, путем установки бэкдора в пакете обновления программного обеспечения M.E.Doc. Одновременно с установкой пакета обновлений на компьютеры учреждений и организаций был установлен бэкдор, способствовавший установке вируса «Petya».

23 мая 2018 года эксперты Cisco предупредили о заражении более 500 000 маршрутизаторов и систем в 54 странах, но главной целью для масштабных кибератак могла быть Украина.[30] Для проведения такой атаки можно использовать деструктивное программное обеспечение «VPN Filter», которое позволяет злоумышленникам перехватывать весь трафик, проходящий через пораженное устройство (включая данные авторизации и персональные данные платежных систем), собирать и выгружать информацию, удаленно управлять зараженным устройством, да еще и вывести его из строя. Также имеются функции для мониторинга протоколов Modbus SCADA, используемых в автоматизированных системах управления.

В предыдущих разделах были оценены все известные кибератаки, повлиявшие на функционирование критических объектов инфраструктуры в энергетическом секторе.

Заключение

В этой статье рассмотрены пути и направления выбора и реализации рациональных подходов к решению комплексной защиты от деструктивного кибер воздействия на государственный энергетический комплекс. Проанализированы все крупные кибератаки на энергетический комплекс Украины в период с 2014 по 2018 год, которые оказали влияние на функционирование объектов критической инфраструктуры в энергетике. Выяснилось, что кибератаки не были одиночными, а проводились систематически. Они оказывали комплексное разрушительное воздействие на системы энергоменедж-

[30] "Global Ransomware Attack Causes Turmoil," *BBC News Ukraine*, June 28, 2017, https://www.bbc.com/news/technology-40416611.

мента. Установлено, что основные деструктивные кибер воздействия сосредоточены на уязвимых элементах (критических узлах) систем управления объектами энергетического комплекса. Перед основной кибератакой проводилась предварительная атака на систему обслуживания и диспетчеризации с целью отказа в обслуживании потребителей. Применение нескольких деструктивных концентрированных кибератак на энергетический комплекс осуществлялось в рамках масштабной кибератаки, направленной на одновременное нарушение работы нескольких объектов энергетики.

Установлено, что система производства и поставки электроэнергии зависит от уровня киберустойчивости энергообъектов. Анализ кибератак показал, что минимальное значение уровня устойчивости может привести к разрушению функционирования энергосистемы (объекта, сети).

Описаны методы реализации гибридных распределенных кумулятивных кибератак с цепным воздействием на объекты критической инфраструктуры. Определены уязвимости этих объектов. Установлено, что кибератаки, осуществленные через электронную почту, обеспечивали доступ к основным серверам для получения информации о состоянии работы системы для перехвата контроля над объектами энергетической инфраструктуры в целом, и затем изменялись параметры их функционирования.

Авторы разработали методику обнаружения гибридных распределенно-концентрированных кибератак с цепными эффектами с использованием модели интеллектуального распознавания киберугроз. Они также разработали организационные и технические меры для обеспечения кибербезопасности в энергетическом секторе. Показано, что систематические меры, направленные на своевременное обнаружение киберугроз, предотвращение и противодействие кибератакам, обеспечат необходимый уровень функциональной устойчивости систем энергокомплекса к деструктивным кибер-воздействиям. Это обеспечит их адекватное реагирование на актуальные и потенциальные угрозы, рационально используя имеющиеся возможности и ресурсы государства.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Издание *Connections: The Quarterly Journal*, том 18, 2019 осуществляется при поддержке правительства Соединенных Штатов.

Об авторах

Тамара Малярчук, кандидат наук, работала в ООО «УкрЭнерджи» с 2016 по 2018 год. Доктор Малярчук был членом рабочей группы НАТО по реализации программы DEEP в Вооруженных силах Украины. Она была аналитиком в Житомирском военном институте им. С. Королева в Украине и работала с американскими военными в области языковой и киберзащиты. Она проводит исследования в области электронного обучения, инновационных технологий в области обнаружения и лечения посттравматического стрессового расстройства, манипулятивных технологий в веб-среде.
E-mail: maliarchuktamara@gmail.com

Генерал-майор **Юрий Даныk**, профессор, доктор технических наук, начальник Института информационных технологий Национального университета обороны Украины им. Ивана Черняховского. Он является экспертом в области военного искусства, национальной обороны и безопасности, информации и кибербезопасности, электронных и ИТ-технологий, проектирования и применения робототехнических комплексов, подготовки спецподразделений. Имеет боевой опыт применения передовых оборонных технологий в условиях современной войны. *E-mail*: zhvinau@ukr.net

Д-р **Чад Бриггс** – доцент и директор департамента государственной политики и администрации Университета Аляски в Анкоридже. Доктор Бриггс имеет практический опыт в области информационных и гибридных войн, а также в разработке оборонительных стратегий для защиты критически важных систем в Восточной Европе и на Балканах. Он имеет докторскую степень в области политологии Карлтонского университета в Канаде, а ранее был старшим советником Министерства энергетики США и программы Минерва, а также профессором по энергетической и экологической безопасности в Академии ВВС США (USAF). Он является автором (вместе с Мириам Матеджовой) книги *«Безопасность при бедствиях: использование разведывательных данных и военного планирования для оценки энергетических и экологических рисков»*. *E-mail*: cbriggs9@jhu.edu