Lir Victor Erikhovich
Candidate of Sciences in Economics, Leading researcher
Department of sectoral forecasts and market conditions
Institute of Economics and Forecasting of NAS of Ukraine

CYBER SECURITY AS A CHALLENGE OF ENERGY DIGITALIZATION

Лір Віктор Еріхович
кандидат економічних наук, провідний науковий співробітник
відділу секторальних прогнозів і кон'юнктури ринків
ДУ «Інститут економіки та прогнозування НАН України»

КІБЕРБЕЗПЕКА ЯК ВИКЛИК ЦИФРОВІЗАЦІЇ ЕНЕРГЕТИКИ

Summary. This paper studies the global problem of cyberterrorism and its relevance for the energy supply system of Ukraine. The most notable hacker attacks and the incurred financial and more general economic costs are examined. The institutional framework for computer security in objects of critical infrastructure is analyzed. Information security risks for Ukraine's energy supply system have been evaluated. The defining features of most contemporary cybercrimes are studied in depth, particularly the evolving motivation and organization of hacker groups. The paper suggests some vectors for improving cybersecurity at the macro- and microeconomic levels to achieve greater energy security in Ukraine.

Анотація. Розглянуто сутність поняття кібертероризму. Наведені факти найбільш масштабних кібератак та оцінки економічних втрат у світовому масштабі. Проаналізовано сучасний стан інституційного забезпечення у сфері інформаційного захисту критичної інфраструктури. Здійснено оцінку існуючого рівня кіберзагроз для системи енергозабезпечення України. Виявлені особливості сучасної кіберзлочинності, зокрема щодо зміни мотивації та способів організації хакерських груп. Запропоновані напрями підвищення кібербезпеки на макро- та мікроекономічному рівнях з точки досягнення національної енергетичної безпеки.

Key words: cyber security, digitalization, critical infrastructure, smart grid, ICT, energy security.

Ключові слова: кібербезпека, цифровізація, критична інфраструктура, інтелектуальна енергетична система, інформаційно-комунікаційні технології, енергетична безпека.

Постановка проблеми. Конвергенція інформаційно-комунікаційних та енергетичних технологій поставила на порядок денний нову проблему захисту інтелектуальних енергетичних систем від цілком реальних кібератак, у більш широкому аспекті – від кібертероризму на об'єктах критичної інфраструктури. Нині кібербезпека все частіше розглядається, як стратегічна проблема державного значення, що зачіпає усі верстви суспільства і тому має стати предметом всебічного наукового дослідження. Державна стратегія кібербезпеки (National Cyber Security Strategy – NCSS) має стати ефективним засобом посилення безпеки та надійності інформаційних систем держави.

Аналіз останніх досліджень і публікацій. В останні роки дослідженням явища кібертероризму приділяється значна увага через проведені кібератаки [1]. Експерти та дослідники звертають увагу перш за все на те, що проблема кібербезпеки зростає з кожним роком і вже найближчим часом може бути співставною за масштабами з проблемою зміни клімату. Світові збитки від кібератак нині перевищують 500 млрд. дол. США. Виходячи з темпів розвитку інформаційно-комунікаційних технологій та динамікою розгортання кіберзлочинності щорічні втрати компаній у глобальному вимірі за експертними оцінками становитимуть до 2021 року вже 6 трлн. дол. США [2]. Згідно доповіді Carbo Disclosure Project (CDP) фінансові збитки у 200 найбільших компаній світу найближчими роками складуть майже 1 трлн. дол. США [3]. Для порівняння за даними World Bank номінальний світовий ВВП у 2018 році становив майже 86 трлн. дол. США.

Дослідники звертають увагу на посилення залежності суспільства від стабільної роботи інформаційних систем. Особливо вразливими для кібератак автори називають ті країни, які не достатньо оснащені програмними та/або технічними засобами власного виробництва. Резонансного характеру вони набувають в тих країнах, які так чи інакше намагаються проводити незалежну політику. Випробування економічної стійкості інфраструктурних систем цих країн провідні фахівці IT галузі пов'язують з випробуваннями нової інформаційної зброї в якості прихованого засобу ведення гібридних війн.

Виділення невирішених частин проблеми. Проблема національної енергетичної безпеки на сучасному етапі розвитку ринків енергоресурсів набуває нового ракурсу у контексті розвитку цифрової енергетики. Зростаючі загрози кібератак на об'єкти енергетики стають особливо небезпечними, якщо мова йде про атомні та гідроелектростанції, трансформаторні підстанції та інше сітьове обладнання, які забезпечують стабільну роботу всієї енергетичної системи країни, а відтак і системи життєзабезпечення країни в цілому.

Мета статті. Метою статті є оцінка існуючого рівня кіберзагроз, оцінка можливих збитків від порушення надійності енергопостачання, оцінка стану інституційного забезпечення у сфері інформаційної безпеки, визначення напрямів підвищення рівня кібербезпеки енергетичної системи країни з точки досягнення прийнятного рівня національної енергетичної безпеки.

Виклад основного змісту

Термін «кібертероризм» був запропонований в 1980-х роках науковим співробітником Інституту безпеки і розвідки (англ. Institute for Security and Intelligence) Баррі Колліном, який використовував його в контексті тенденції переходу тероризму з фізичного у віртуальний світ, зростаючого перетину і зрощення цих світів [4]. Центр стратегічних і міжнародних досліджень (США) визначає кібертероризм як «використання комп'ютерних мережевих інструментів для припинення функціонування критичних об'єктів національної інфраструктури (зокрема, енергетичних, транспортних, урядових), або для залякування уряду чи цивільного населення» [5].

Проведений аналіз явища кібертероризму показує, що до його особливостей відносяться: 1) кібертероризм є інформаційною зброєю, так як використовує комп'ютерні системи та мережі, спеціальне програмне забезпечення та інформаційні технології; 2) кібертероризм носить міжнародний характер, оскільки злочинці знаходяться в одній державі, а їх жертви за кордоном; 3) кібертероризм має різноманітні цілі; 4) кібертероризм характеризується високим рівнем латентності й низьким рівнем розкриття; 5) кібертероризм потребує порівняно невеликих фінансових витрат але завдає величезних матеріальних збитків [6].

У 2006 році провідними країнами світу було ініційовано розробку оновлених міжнародно-правових документів щодо боротьби з кібертероризмом. Це дало важливий сигнал усій світовій спільноті і призвело до створення національних і міждержавних підрозділів, діяльність яких спрямована на боротьбу з кібертероризмом. Так, 18 січня 2013 року в Гаазі офіційно відкритий Європейський центр по боротьбі з кіберзлочинністю. Він здійснює збір і обробку даних про кіберзлочини, надає експертну оцінку інтернет-загрозам, а також розробляє та впроваджує передові методи профілактики і розслідування кіберзлочинів.

Відповідно до стандарту X.1205 (04/2008) Міжнародного союзу електрозв'язку [7] кібербезпека визначається як набір засобів, стратегій, принципів досягнення безпеки; гарантії безпеки; керівні принципи та підходи до управління ризиками; дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації і користувача. *Ресурси організації і користувача* включають під'єднані комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи електрозв'язку і всю сукупність переданої і/або збереженої інформації в кіберсередовищі. Кібербезпека полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. У свою чергу *кіберсередовище* включає: користувачів, мережі, пристрої, все програмне забезпечення, процеси, збережену або транзитну інформацію, програми, служби та системи, які можуть бути прямо або опосередковано пов'язані з мережами.

За даними звіту Міжнародного союзу електрозв'язку щодо Глобального індексу кібербезпеки (Global Cybersecurity Index (GCI)) за 2018 рік Україна посідає 54 місце у загальному (серед 175 країн світу) та 33 місце у регіональному (європейському, серед 43 країн) рейтингу з кібербезпеки [8]. У 2018 році кількість країн, що мають інституційне забезпечення кібербезпеки та відповідальність за кіберзлочини збільшилася з 71% до 91%. Також збільшилася кількість країн, що мають Національну стратегію з кібербезпеки. Серед головних факторів, які враховуються при визначення індексу GCI названі з рівними ваговими коефіцієнтами (0,2) наступні: інституційне забезпечення, технічне забезпечення, організаційні заходи, кваліфікація (цифрові компетенції) персоналу, рівень співробітництва, а також рівень комунікації та кооперації. В цілому Україна відноситься до групи країн із середнім рівнем кібербезпеки, хоча і посідає третю сходинку у цій групі після Узбекистану та Молдови. Натомість, такі країни як Грузія, Казахстан, В'єтнам та Уругвай входять до групи з високим ступенем кібербезпеки.

Робочою групою CIGRE (Міжнародна Рада з великих електричних систем великої напруги) були сформульовані вимоги до кібербезпеки (The Impact of Implementing Cyber Security Requirements using IEC 61850), основними з яких є: управління доступом (AC – Access Control) – для захисту від несанкціонованого доступу до пристрою або інформації; управління використанням (UC –Use Control) – для захисту від несанкціонованого оперування або використання інформації; цілісність даних (DI – Data Integrity) – для захисту від несанкціонованої зміни; конфіденційність даних (DC –Data Confidentiality) – для захисту від несанкціонованого доступу; обмеження потоку даних (RDF –Restrict Data Flow) – для захисту від публікації інформації на несанкціонованих джерелах; своєчасна відповідь на подію (TRE – Timely Responseto Event), моніторинг і протоколювання даних пов'язаних з безпекою [9].

Останніми роками Україна також здійснила певні кроки у формування інституційного середовищу у сфері інформаційної безпеки. Указом Президента України від 16 березня 2016 р. затверджена Стратегія кібербезпеки України [10], яка попередньо була схвалена рішенням РНБО України. Метою документа є створення умов для

безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. Основу національної системи кібербезпеки складає Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Стратегія передбачає створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору і досягнення сумісності з відповідними стандартами ЄС і НАТО, а також надання послуг із захисту інформації та кіберзахисту. При цьому до підготовки проектів концептуальних документів у цій сфері залучається експертний потенціал наукових установ, професійних і громадських об'єднань. Також Стратегією передбачено підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі, а також розвиток міжнародного співробітництва та підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співробітництва України з ЄС та НАТО. Також створено Національний координаційний центр кібербезпеки як робочий орган РНБО.

За даними компанії Positive Technologies серед усіх кібератак на промислові об'єкти у світі в 2018 році 77% припадало на об'єкти інфраструктури (49% від загальної кількості атак) [11]. Необхідність посилення рівня кібербезпеки в реальному секторі економіки зумовила розробку та прийняття Закону України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 5 жовтня 2017 року. В цьому Законі термін «критично важливі об'єкти інфраструктури» (далі – об'єкти критичної інфраструктури) визначається як «підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей». Цей Закон також надає взаємопов'язане визначення «об'єкта критичної інформаційної інфраструктури», як «комунікаційної або технологічної системи об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури» [12].

Реалізація концепції інтелектуальних енергетичних мереж призводить до нових ризиків та загроз з точки зору інформаційної безпеки, зокрема: підвищення складності електричної мережі у свою чергу підвищує рівень вразливості для потенційних атак та непередбачуваних помилок в управлінні; інтеграція через інформаційні канали енергетичних мереж різного рівня ієрархії підвищує ризики розгортання каскадних аварій; велика кількість взаємопов'язаних сітьових програмних компонентів підвищує вразливість програмного коду до проникнення та розповсюдження шкідливих кодів; збільшення вузлових точок інтелектуальної мережі збільшує точки входу для вірусних програмних продуктів [13].

Необхідність розробки національного інституційного середовища та комплексу взаємоузгоджених заходів з кібербезпеки стала зрозумілою після перших кібератак на енергетичну систему країни. Перша зареєстрована успішна кібератака на енергетичну систему України з виведенням її із ладу сталася 23 грудня 2015 р., коли зловмисникам вдалося успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній. Внаслідок атак відбулося відключення напруги на семи підстанціях 110 кВ і двадцяти трьох підстанціях 35 кВ, що призвело до відключення енергопостачання в 5 регіонах країни на 6 годин. Біля 230 тисяч мешканців залишались без світла протягом однієї-шести годин.

В ході атак були вчинено: зміни конфігурації RTU (програмно-апаратні пристрої середнього рівня автоматичних систем управління технологічними процесами - АСУ ТП); знищена інформація на АРМ (автоматизованих робочих місцях) диспетчерського персоналу; DDoS-атаки (атаки, спрямовані на відмову в обслуговуванні), які зазнали call-центри енергопостачальних компаній [14]. Кібератака на енергетичну інфраструктуру України в 2015 році була останньою операцією з використанням набору інструментів Black Energy.

Найбільша кібератака сталася в Україні 27 червня 2017 року через розповсюдження вірусу Petya.A, який втрутився у діяльність сотень компаній і заблокував роботу тисяч персональних комп'ютерів (за деякими даними, одну десяту всіх комп'ютерів в державному та корпоративному секторі). За експертними оцінками, сумарні збитки від цього руйнівного вірусу склали майже 0,5% ВВП всієї країни, або 14 мільярдів гривень [15].

Згідно з висновками експертів ESET, які займалися розслідуванням попередніх кібератак на Україну, хакери вже змогли успішно встановити на комп'ютери по всьому світу шкідливий програмний код, який в певний момент зможе дозволити зловмисникам взяти контроль над усіма інфікованими пристроями та/або використовувати їх для потужної атаки. Кінцева мета всіх цих приготувань поки невідома, як і немає точної відповіді на те, хто замовник інформаційної війни. Але можна констатувати, що нова зброя вже розроблена і продовжує стрімко удосконалюватися.

Фахівці з ESET знайшли докази зв'язку цього шкідливого програмного забезпечення, названого Grey Energy, з хакерською групою TeleBots і

вірусами групи Black Energy, які раніше вже атакували Україну. Згідно з висновками британської розвідки і Служби безпеки України (яка проводила розслідування попередніх атак за підтримки американських спецслужб), джерелом згаданих нападів була Росія. І хоча фахівці ESET, також брали участь в розслідуванні цифрової агресії проти українців, не підтверджують але і не спростовують «російський слід», можна припустити, що Україна стикається з черговим проявом гібридної війни в інформаційному просторі.

Останні два роки фахівці IT індустрії звертають увагу та попереджають про зростаючий рівень загроз кібератак для України, які перш за все можуть бути спрямовані на енергетичну систему країни як об'єкт критичної інфраструктури. Співробітники антивірусної компанії ESET зафіксували нову APT-підгрупу (від англ. Advanced Persistent Threat –«розвинена стійка загроза»; також цільова кібератака) – TeleBots. Вона стала відомою завдяки глобальному поширенню NotPetya–шкідливого програмного забезпечення, яке порушило глобальні бізнес-операції в 2017 р. і привело до збитків на мільярди доларів. Як підтвердили дослідники, TeleBots також пов'язана з Industroyer, потужною сучасною шкідливою програмою, націленою на промислові системи управління, яка викликала друге припинення електропостачання в Україні в 2016 р. [16]. Ця аварія була менш масштабною за наслідками, оскільки відбулась вночі з 16 на 17 грудня 2016 року [17]. Протягом однієї години була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», без струму залишились споживачі північної частини правого берега м. Києва та прилеглих районів області.

У лютому 2019 року аналітична компанія Counterpoint Technology Market Research представила десять прогнозів у сфері інформаційної безпеки на 2019 рік, зокрема щодо загроз та контрзаходів (табл.1).

Таблиця 1.

Актуальні тенденції кібербезпеки

Загрози	Контрзаходи
Зміцнення співробітництва між згуртованими у злочинні групи хакерами(APT-групи) та хакерами-фрілансерами	Співробітництво та розширення партнерських зв'язків між розробниками антивірусних рішень
Поширення ринку послуг на хакерські атаки під замовлення третіх клієнтів	Багатофакторна аутентифікація та інтелектуальна ідентифікація пристроїв
Використання технологій штучного мислення для подолання бар'єрів, створених попередніми версіями штучного інтелекту	Випереджаючий розвиток захисних технологій машинного навчання (штучного інтелекту)
Зростання обсягів крадіжок даних з хмарних сховищ	Вбудоване в апаратну частину оригінальне захисне програмне забезпечення
Дестабілізація роботи «розумних міст» та з метою створення панічних настроїв	Зростання попиту на фахівців ITсектору

Джерело: складено за даними Counterpoint Technology MarketResearch Режим доступу: http://www.tadviser.ru/index.php

Отже сучасна кіберзлочинність постійно модифікує свою діяльність. Зміни стосуються як мотивації до здійснення кіберзлочинів, так і напрямів кібератак. Кіберзлочинність у сучасному світі представляє собою не меншу загрозу для розвитку цивілізованого суспільства ніж тероризм у фізичному (реальному) вимірі. Це серйозний супротивник, що має високий рівень спеціальних знань і значні ресурси, які дозволяють йому досягати цілей за допомогою різних векторів нападу: інформаційних, фізичних і обманних. Зловмисники прагнуть встановити контроль усередині інформаційної-технологічної інфраструктури, здійснити підрив або створити перешкоди для виконання її завдань. Так само злочинці можуть зайняти вичікувальну позицію, щоб здійснити ці наміри в майбутньому3. Боротьба з такими злочинними групами можлива лише із залученням потужних інтелектуально-фінансових ресурсів в рамках державно-приватного партнерства з міжнародними IT-компаніями.

Висновки та перспективи досліджень

Конвергенція інформаційних та енергетичних технологій поставила на порядок денний проблему захисту інтелектуальних енергетичних систем від кібератак. У розвинутих країнах світу кібербезпека енергетичних систем розглядається, як стратегічна проблема національної безпеки. Сучасна кіберзлочинність дуже швидко адаптується до зростання геополітичних та економічних конфліктів і наразі вже не фокусується на фінансових крадіжках у системах інтернет-банкінгу, комерційному шпіонажі або прямому нанесенні збитків конкурентам. Потужні хакерські групи переходять на мезо- та макрорівень, здебільшого спрямовують атаки на системи захисту

3Режимдоступу: https://www.unian.net/science/10309830-ekspert-po-kiberbezopasnosti-robert-lipovski-osnovnaya-gipoteza-ukraina-ispolzuetsya-kak-testovaya-ploshchadka-gruppami-hakerov-na-vashey-strane-oni-testiruyut-svoy-arsenal-kiber-oruzhiya.html

інформації та економічний потенціал країни, перш за все на об'єкти критичної інфраструктури. Боротьба з такими злочинними групами можлива лише із залученням потужних інтелектуально-фінансових ресурсів, державної підтримки та формування міжнародних консорціумів антивірусних компаній.

На рівні корпорацій потрібно радикально переглянути організаційну структуру компаній та запровадити окремий відділ з кібербезпеки та запровадити посаду заступника директора з інформаційної безпеки. В уставі компанії необхідно чітко визначити види даних та їх носіїв, які мають першочергове значення для фізичної, інформаційної та економічної безпеки компанії (конкурентоспроможності). На рівні компанії має бути розроблено та затверджено правлінням бізнес-план з кібербезпеки. На світовому ринку все більш поширеною практикою при створенні (замовленні) програмного забезпечення стає інсорсінг. Персонал компанії має бути чітко обізнаний з правилами інформаційної безпеки, зокрема щодо дублювання важливих даних на альтернативних носіях та пристроях, ігнорування запитів соціальної інженерії, оновлення антивірусного комплекту та періодичний огляд файлової системи (так звана елементарна інформаційна профілактика).

Перспективними напрямами підвищення рівня кібербезпеки у сфері енергетики є активізація міжнародного науково-технічного співробітництва у сфері інформаційної безпеки між країнами, які знаходяться у стадії інтеграції національних енергетичних систем, зокрема між Україною та країнами Східної Європи. Актуальними завданнями такого співробітництва постають: розробка єдиних стандартів кібербезпеки, співробітництво між службами кіберполіції, організація спільних навчальних програм персоналу компаній з підвищення рівня цифрових компетенцій тощо.

Список літератури

1. Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности, №5(8) – 2014. – С. 30-38. URL: http://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya/viewer
2. Ежегодно компании теряют от кибератак до 6 триллионов долларов США. URL: http://channel4it.com/publications/Ezhegodno-kompanii-teryayut-ot-kiberatak-do-6-trillionov-dollarov-SSHA-35900.html
3. Ущерб от изменения климата составит более $1 трлн. URL: https://www.meteovesti.ru/news/63695318064-uscherb-izmeneniya-klimata-sostavit-bolee-1-trln
4. Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. – 1997. – Vol.13.
5. Lewis J. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
6. Кибертерроризм: угроза национальной и международной безопасности. URL: https://www.arms-expo.ru/news/archive/kiberterrorizm-ugroza-nacional-noy-imezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/
7. ITU-T Rec. E.164 / I.331 / Q.11 (02/2005) The international public telecommunication numbering plan
8. Global Cyber security Index (GCI) 2018 / ITU Publications. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
9. Массель Л.В. Использование современных информационных технологий в Smart Grid как угроза кибербезопасности энергетических систем России // Information Technology and Security № 1(3) – 2013. - С.56-65.
10. Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL:https://zakon5.rada.gov.ua/laws/show/96/2016
11. Актуальные киберугрозы — 2018. Тренды и прогнозы / Positive Technologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf
12. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
13. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности №4(17). – 2016. – С.2-9. URL: https://cyberleninka.ru/article/v/kiberopasnost-kak-odna-iz-strategicheskih-ugroz-energeticheskoy-bezopasnosti-rossii
14. SANS-ICS, E-ISAC. TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)
15. Эксперты оценили потери от вируса Petya.A в 0,5% ВВП Украины. URL: https://tsn.ua/ru/ukrayina/eksperty-ocenili-poteri-ot-virusa-petya-a-v-0-5-vvp-ukrainy-890153.html URL: https://tsn.ua/ru/ukrayina/eksperty-ocenili-poteri-ot-virusa-petya-a-v-0-5-vvp-ukrainy-890153.html
16. Герман Б. Украина стала плацдармом для кибератак / Дзеркало тижня 3 листопада, 2018. URL: https://zn.ua/business/ukraina-stala-placdarmom-dlya-kiberatak-299046_.html
17. Kim Zetter (January 10, 2017). The Ukrainian Power Grid Was Hacked Again. URL: https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report