4. Spickernell S. Muslims are disproportionately likely to become company directors [Electronic resource] / City A.M. – Regime to access: http://www.cityam.com/210932/least–third–uk–company–directors–are–muslim–which–much–higher–proportion–muslims–society (05.03.2015). – Title from screen.

5. В Великобритании находятся 23 тысячи потенциальных террористов [Электронный ресурс] / Islam–today. – Режим доступа: http://islam–today.ru/novosti/2017/05/29/v–velikobritanii–nahodatsa–23–tysaci–potencialnyh–terroristov/ (29.05.2017). – Название с экрана.

6. Дебрер С. «Исламский фактор» разделил Германию [Электронный ресурс] / Свободная Пресса. – Режим доступа: http://svpressa.ru/world/article/148377/ (12.05.2016). – Название с экрана.

7. Меркель рассказала в Мюнхене про серьезные вызовы для демократии [Электронный ресурс] / News24.ua. – Режим доступа: http://news24ua.com/merkel–rasskazala–v–myunhene–pro–sereznye–vyzovy–dlya–demokratii (18.02.2017). – Название с экрана.

References

1. Sumlenniy S., Koksharov A. Teper zdes islam [Elektronniy resurs] / Ekspert Online. – Rezhim dostupa: http://expert.ru/expert/2008/38/teper_zdes_islam/ (29.09.2008). – Nazvanie s ekrana.

2. Gashkov I. Musulmane reshayut sudbu vyborov vo Frantsii [Elektronniy resurs] / RIA Novosti. – Rezhim dostupa: https://ria.ru/world/20170417/1492433937.html (17.04.2017). – Nazvanie s ekrana.

3. Religion in England and Wales 2011 [Text] / Office for National Statistics. – 11 December 2012. – 12 p.

4. Spickernell S. Muslims are disproportionately likely to become company directors [Electronic resource] / City A.M. – Regime to access: http://www.cityam.com/210932/least–third–uk–company–directors–are–muslim–which–much–higher–proportion–muslims–society (05.03.2015). – Title from screen.

5. V Velikobritanii nahodiatsia 23 tysiachi potentsialnyh terroristov [Elektronniy resurs] / Islam–today. – Rezhim dostupa: http://islam–today.ru/novosti/2017/05/29/v–velikobritanii–nahodatsa–23–tysaci–potencialnyh–terroristov/ (29.05.2017). – Nazvanie s ekrana.

6. Debrer S. «Islamskiy faktor» razdelil Germaniyu [Elektronniy resurs] / Svobodnaya Pressa. – Rezhim dostupa: http://svpressa.ru/world/article/148377/ (12.05.2016). – Nazvanie s ekrana.

7. Merkel rasskazala v Miunhene pro sereznie vyzovy dlia demokratii [Elektronniy resurs] / News24.ua. – Rezhim dostupa: http://news24ua.com/merkel–rasskazala–v–myunhene–pro–sereznye–vyzovy–dlya–demokratii (18.02.2017). – Nazvanie s ekrana.

Vonsovych O. S., *PhD in Political Science, associate professor of international relations department of Private Joint Stock Company «Higher educational institution «University of Central Europe» (Ukraine, Kyiv), sefinrof@ipnet.ua*

The influence of the Islamic factor on the European security system

The purpose of this article is to investigate the causes of the influence of the Islamic factor on the European security system. During writing, the author used the following methods: analysis, synthesis, comparison, induction, deduction. The main obtained conclusions are as follows: today the role of the Islamic factor in European affairs is quite tangible: first of all, this is manifested in the fact that the increasingly active Muslim diaspora begins to interfere in the internal affairs of the leading European countries, which today define the general policy of the European Union; the leveling of European interests can lead to unforeseen consequences, one of which may be the so–called «Islamization» of Europe; important for Europe remains the issue of combating against various manifestations of terrorist activity: the key aspect should remain a departure from the liberal, democratic principles of combating against actual challenges and threats, and the transition to military actions using international support in the face of NATO.

Keywords: *Islamic factor, European security system, European Union, terrorism, challenges, threats.*

* * *

УДК 324

Дубов Д. В.,
доктор політичних наук, старший науковий співробітник, завідувач відділу інформаційної безпеки та розвитку інформаційного суспільства, Національний інститут стратегічних досліджень (Україна, Київ), shamus123@ukr.net

Дубова С. В.,
кандидат історичних наук, викладач кафедри інформаційної, бібліотечної та архівної справи, Київський національний університет культури і мистецтв (Україна, Київ), sdubova@ukr.net

«СОЦІАЛЬНІ КІБЕРАТАКИ» ЯК ІНСТРУМЕНТ ХАОТИЗАЦІЇ ПОЛІТИЧНИХ ПРОЦЕСІВ (НА ПРИКЛАДІ ВИБОРЧОГО ТА ПОСТВИБОРЧОГО ПЕРІОДУ В США У 2016–2017 РР.)

Досліджено «соціальні кібератаки» як інструмент хаотизації політичних процесів (на прикладі виборчого та поствиборчого періоду в США у 2016–2017 рр.). За результатом дослідження робиться висновок, що за останні 25 років США чи не вперше зіткнулись із дійсно серйозним викликом власній політичній безпеці, який походить з кіберпростору. Мета акцій деструктивного кібервпливу полягала не у прямій дискредитації виборів, а компрометації та хаотизації політичного процесу як такого. Ця мета в цілому була досягнута, адже нове керівництво держави виявилось скомпрометованим вже на початку своєї каденції. Завдяки кібератакам вдалось дестабілізувати функціонування політичної системи країни із значними політичними традиціями, відпрацьованими практиками передачі влади та чітко функціонуючими демократичними інститутами. В подальшому соціальна складова кібер атак буде лише зростати.

Ключові слова: *кібератаки, вибори, США, хаотизація, політичний процес, РФ.*

Проникнення інформаційних технологій у всі сфери життя суспільства досягло рівня, коли їх протиправне використання може бути застосоване не лише для кіберзлочинних (передусім – фінансових), шпигунських чи диверсійних (проти критичної інфраструктури) цілей, але і як інструмент впливу на політичні процеси іншої держави. Сьогодні, коли експерти як в Україні, так і на кажуть про те, що Російська Федерація розгорнула масштабну світову гібридну війну проти світу [18], ця проблема постає з особливою актуальністю саме в цьому контексті. Особливо зважаючи на те, що методи своєї деструктивної діяльності РФ черпає з досвіду холодної війни та практики «активних заходів» (як в сьогоднішній російській розвідувальній дійсності мають назву «заходи сприяння»). Як зазначають автори доповіді «Активні заходи» СРСР проти США: пролог до гібридної війни»: «Підпорядкованість єдиному задуму сукупності застосовуваних методів тиску на інші держави є ознакою розгортання «активних заходів» (англ. – active measures) – практики, що постала з діяльності радянських спецслужб. Дезінформація, агенти впливу, квазігромадські організації, інформаційний тиск стали системними реаліями того часу. Сьогодні ця практика знов на порядку денному. Часто навіть у тих самих формах» [14, с. 6].

Одним з таких інструментів на нинішньому етапі визнається і використання кібератак, які мають на меті вплинути на політичний процес в інших державах, дестабілізувати їх, зменшити політичну єдність сил держави, трансформувати їх стратегічні пріоритети. Тому сьогодні все частіше кажуть про так–звані «соціальні кібератаки» [11] – кібератаки, які мають не стільки технічний вимір (очікуваний деструктивний наслідок для інформаційно–телекомунікаційної системи),

скільки суспільно–політичний або соціальний і забезпечують процес втручання у виборчий процес для досягнення стратегічної мети ініціатора кібератаки. Таке втручання більшою мірою хаотизує політичний процес, зменшуючи стійкість держав до сторонніх впливів та дезорганізуючи їх стратегічну діяльність. Президентські вибори в США в 2016 році (а потім – і процес розслідування втручання в них РФ) стали одним з найпоказовіших прикладів таких «соціальних кібератак».

Сьогодні деструктивна діяльність у кіберпросторі, як елемент впливу на політичні процеси, розглядається, переважно, в межах дослідження концепції гібридної війни. Окремі аспекти висвітлено в колективній монографії «Світова гібридна війна» колективу Національного інституту стратегічних досліджень, публікаціях В. Горбуліна, Д. Дубова, М. Ожевана, С. Гнатюка, В. Петрова, В. Гусарова, Д. Золотухіна. Питанню кібервтручання у вибори президента США присвячено цілу низку робіт американських дослідників: Е. Осноса, Д. Ремніка, Дж. Йаффа. Однак цілісні дослідження, які б узагальнили відомості про вплив «соціальних кібератак» на політичний процес все ще відсутні.

Мета дослідження – дослідити вплив «соціальних кібератак» як інструменту хаотизації політичних процесів (на прикладі виборчого та поствиборчого періоду в США у 2016–2017 рр.).

У липні 2016 року WikiLeaks опублікував відомості про 20 тисяч листів Національної демократичної партії США, з яких стало відомо, що партія приховано «грала» на користь Х. Клінтон (як кандидата від Демократичної партії) та проти її конкурентів по праймеріз. Тоді це призвело до того, що один з помітних функціонерів партії – Д. Вассерман–Шульц – пішла у відставку. Також в цих листах йшлося про системний збір демпартією інформації про основного кандидата від республіканців – Д. Трампа.

Для Сполучених Штатів, де позиціям кандидатів з тих чи інших питань приділяється величезна увага, де питання «моральної чистоти» та хоча б показової «чесності» ведення кампаній надається великого значення, подібні викриття стали дійсно серйозним випробуванням. Більшу частину літа 2016 року Демпартія США виправдовувалась і намагалась знайти винних і в цьому контексті частіше за все згадували РФ. І представники Демпартії США [14], і окремі посадовці [13] почали називати замовником атаки РФ, адже на їх думку ця атака була здійснена в інтересах перемоги Д. Трампа якого вважали більш лояльним до В. Путіна та політики РФ кандидатом. Судячи з тих даних, які наявні зараз завдяки звітам контррозвідувальних та розвідувальних органів США, такі припущення були обгрунтованими.

Вірус потрапив у інформаційну мережу Демпартії класичним фішинговим методом, коли заражений електронний лист було надіслано одному з співробітників Національного комітету Демократичної партії США. Відкривши його розробники вірусу змогли розвинути свій успіх, наслідком якого став злам більше 100 електронних поштових ящиків окремих посадових осіб та відділень партії. В Демпартії помітили неправильну роботу інформаційних систем лише у травні 2016 року.

На тому етапі реакція держави на ці злами була досить неоднозначною. Як частину такої відповіді можна розглядати підписання Б. Обамою 26 липня 2016 року політичної директиви (Presidential Policy Directive) спрямованої на встановлення чіткого механізму координації відомств для відповіді на кібератаки [8]. Ця директива встановлює керівні принципи такої відповіді:

1. Спільна відповідальність (окремі громадяни, бізнес сектор та держава мають спільний інтерес у захисті держави від кібератак).

2. Відповідь на основі ризиків (відповідь має бути еквівалентна тим ризикам, які несе кібератака для національної безпеки, міжнародних відносин, економіки, додержання правил державної таємниці, громадянських свобод чи здоров'я та безпеки американських громадян).

3. Повага/врахування інтересів постраждалих (відзначається, що Уряд буде захищати деталі інциденту, захищати персональні дані його учасників, а також чутливу інформацію бізнес структур).

4. Єдність відповіді уряду на атаку (різні відомства мають різні можливості та різні повноваження реагувати на кібератаки, однак у разі її виявлення всі вони мають максимально повно включатись у забезпечення відповіді та ефективно координуватись в цьому питанні).

5. Сприяння швидкому відновленню постраждалого об'єкта (передусім – через оптимізацію проведення розслідування в такому режимі, що б воно дозволяло об'єкту атаки якомога скоріше повернутись до повноцінної роботи).

Крім того, цей документ встановлює порядок координації на державному рівні дій федеральних структур, визначаючи при цьому роль окремих підрозділів Ради національної безпеки США та Міністерства юстиції (що діє через ФБР).

За наявними даними [4] за зламом Демпартії США стояли два угрупування хакерів – Fancy Bear та Cozy Bear. Обидві вважають російськими хакерськими угрупуваннями, які тісно пов'язані із російськими спецслужбами. Визначаючи їх взаємовідносини із розвідувальними органами РФ експерти визначають [2] їх як вільнонайманими хакерами на державній службі. Fancy Bear приписують атаки на інформаційну систему Бундестагу, атаки на ЗМІ Туреччини на фоні загострення російсько–турецьких відносин, атака в 2015 році на французький телеканал TV5Monde, спроба зламу інформаційної системи Ради безпеки Нідерландів для отримання інформації про розслідування щодо МН17 та інші. Україна також добре відома з діяльністю цього угрупування. Як ви пам'ятаєте наприкінці 2015 року була проведена кібератака на Прикарпаттяобленерго, внаслідок якої на 3 години декілька сотень тисяч громадян України залишились без світла. Cozy Bear відома трохи менше, але також декілька разів згадувалась у ситуації із зламом електронної пошти Пентагону у 2015 році.

Злам Демпартії США було частиною широких зусиль РФ із втручання у американські вибори: Cozy Bear зламала системи Демпартії ще в 2015 році, а – Fancy Bear у квітні 2016–го. Тобто акція готувалась заздалегідь і атака була добре продуманою.

Ця атака стала лише частиною куди більших зусиль з боку РФ із втручання у американські вибори.

Наприклад, незадовго до дня виборів стало відомо про два випадки зламу бази даних виборців які знаходяться, зокрема, в Арізоні та Іллінойсі [12]. Висловлювалось припущення, що якщо хакери знищать ці бази в день голосування, вони можуть завдати дійсно серйозного удару по виборам і поставити їх результати під сумнів. І хоча для цього є певні запобіжники, що мінімізують такі ризики, але небезпека все одно залишається. Наприклад, у штаті Джорджія для голосування використовуються машини для голосування які не мають системи підтвердження паперовими копіями. Вочевидь, розвідувальні структури РФ були добре обізнаними із проблемами із технічним захистом тих інформаційно–телекомунікаційних систем, які використовувались для виборчого процесу. Згідно із таємним звітом АНБ США (який потрапив до преси внаслідок діяльності одного з підрядників цього агентства) [9], за декілька днів до виборів президента США російські спецслужби (вказується, що відповідальність за це може нести ГРУ ГШ РФ) атакували як мінімум одного з американських постачальників програмного забезпечення для проведення виборів.

Цікаво, що позиція російського керівництва щодо причетності РФ до цих атак змінювалась практично так само, як і щодо участі РФ в окупації Криму – від цілковитого заперечення, до часткового визнання і до раптового прийняття. В 2016 році, під час виступу на пленарній сесії щорічного засідання дискусійного клубу «Валдай» на питання щодо втручання РФ у американські вибори жорстко відмітив, що «США – не бананова республіка», щоб допускати втручання у свої вибори [14]. На противагу цьому, в 2017 році під час спілкування з представниками міжнародної преси на щорічному форумі в Санкт–Петербурзі він сказав, що теоретично це могли робити «патріотично налаштовані хакери»: «Якщо вони [хакери] патріотично налаштовані, вони починають вносити свій вклад у боротьбу проти тих, хто погано відгукується по осію. Це можливо? Теоретично можливо» [16].

Стратегічною метою російських хакерів була не в тому, щоб зіграти на стороні республіканців чи демократів – стратегічною метою була хаотизація виборчого (та поствиборчого) процесу як такого. Багато в чому, така мета була досягнута. Навіть під час виборів, ці атаки істотно вплинули на характер передвиборчих кампаній та якість політичних комунікацій в американському суспільстві: політичні передвиборчі заготовки обох партій та логіка боротьби між ними була багато в чому «зламана» і змістилась у сферу виправдань та взаємних звинувачень, а дискусії щодо вини/невиновності зовнішніх гравців у цьому зламі істотно змінили як порядок денний передвиборчих кампаній, так і логіку політичної боротьби.

Однак слід зазначити, що такі впливи є не чимось принципово новим для американо–російських (раніше – американо–радянських) відносин. Автори доповіді [14] відмічають, що ще у 60–і роки 20–го сторіччя КДБ намагався впливати на передвиборчі перегони у США (проти одного з кандидатів – Б. Голдвотера, звинувачуючи його у цинізмі), а у 80–і роки такий вплив став дійсно масштабним. Особливо жорстко та масштабно СРС намагався не допустити обрання на посаду Президента США Р. Рейгана. Для цього радянські розвід служби проникали проникнути в штаб–квартири національних комітетів демократів і республіканців, популяризувати салоган «Рейган означає війна» та дискредитувати Р. Рейгана як «корумпованого службовця, тісно пов'язаного з американським оборонно–промисловим комплексом» [7]. У 1984 році М. Хамм (Manfred R. Hamm) із Фонду «Спадщина» підготував окремий звіт «Як Москва втручається у вибори на Заході» [6], в якому зазначає, що в 1983 році Кремль ставав активним «учасником» виборів у Великій Британії та Західній Німеччині, а в 1984 році почав втручатися в американські вибори. Зокрема, СРСР доклав максимальних зусиль, щоб донести до американської, європейської та світової громадськості думку про те, що американська військова та зовнішньополітична лінія провокують світову нестабільність та конфліктність.

Хоча внаслідок кібератак, самі результати голосування не були поставлені під сумнів, однак це стало початком більш широкого процесу дослідження ступеню впливу РФ на американські вибори. Тим більше, що американську розвідку про посилення кібервтручання російських хакерських груп в американські вибори попереджали розвідки інших держав – передусім партнери по програмі «П'ять очей», а також Німеччина, Естонія та Польща [3].

Починаючи з грудня 2016 року розвідувальні та контррозвідувальні органи США починають озвучувати своє занепокоєння рівнем втручання РФ у американські вибори. Зокрема, 9–го грудня ЦРУ повідомило про втручання законодавців [10], 29 грудня аналогічну позицію було висловлено у офіційному звіті ФБР та Департаменту внутрішньої безпеки [5]. Ці розслідування продовжились і в 2017 році, коли почали з'являтись все нові факти такого втручання [1].

Висновок. Як вже зазначалось мета цих акцій деструктивного кібервпливу полягали не стільки у прямій дискредитації виборів, скільки компрометації та хаотизації політичного процесу як такого. Ця мета в цілому була досягнута, адже США і в 2017 році так і не змогла фактично вийти з виборчого циклу, а нове керівництво держави виявилось скомпрометованим вже на початку своєї каденції. Технічно не складним кібератакам у виконанні російських розвідувальних структур та залучених ними хакерських угрупувань вдалось дестабілізувати функціонування політичної системи країни із значними політичними традиціями, відпрацьованими практиками передачі влади та чітко функціонуючими демократичними інститутами.

За останні 25 років США чи не вперше зіткнулись із дійсно серйозним викликом власній політичній безпеці, який до того ж походить зі сфери, в якій вони традиційно почуваються впевнено – з кіберпростору. РФ вдало використовує офіційні демократичні процедури та переваги Заходу проти нього самого, перекручуючи їх зміст (як це зараз відбувається із свободою слова), або експлуатуючи у власних інтересах (як це було із декількома референдумами у європейських країнах).

Це суперництво все впевненіше набуває рис Холодної війни 2.0. яка хоч і має всі ознаки традиційної холодної війни, однак розгортається у інших просторах.

А це означає подальше збільшення політично значимих кіберінцидентів, а у найбільш радикальних випадках – перехід від кібершпигунства до вкрай небезпечної кібердиверсійної роботи країн. При цьому соціальна складова цих атак буде лише зростати, так само як зростали протягом всього періоду холодної війни інформаційні складові дезінформаційної роботи Радянського Союзу.

Список використаних джерел

1. Background to «Assessing Russian Activities and Intentions in Recent US Elections»: The Analytic Process and Cyber Incident Attribution [Електронний ресурс]. – Режим доступу: https://www.dni.gov/files/documents/ICA_2017_01.pdf
2. Bears in the Midst: Intrusion into the Democratic National Committee [Електронний ресурс]. – Режим доступу: https://www.crowdstrike.com/blog/bears–midst–intrusion–democratic–national–committee/
3. British spies were first to spot Trump team's links with Russia [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/uk–news/2017/apr/13/british–spies–first–to–spot–trump–team–links–russia
4. Cyber researchers confirm Russian government hack of Democratic National Committee [Електронний ресурс]. – Режим доступу: https://www.washingtonpost.com/world/national–security/cyber–researchers–confirm–russian–government–hack–of–democratic–national–committee/2016/06/20/e7375bc0–3719–11e6–9ccd–d6005beac8b3_story.html?utm_term=.3946064d9257
5. Grizzly steppe – Russian Malicious Cyber Activity [Електронний ресурс]. – Режим доступу: https://www.us–cert.gov/sites/default/files/publications/JAR_16–20296A_GRIZZLY%20STEPPE–2016–1229.pdf
6. Manfred R. Hamm. How Moscow Meddles in the West's Elections [Електронний ресурс]. – Режим доступу: http://s3.amazonaws.com/thf_media/1984/pdf/ bg369.pdf
7. Osnos E., Remnick D., Yaffa J. Active measures: What lay behind Russia's interference in the 2016 election—and what lies ahead? // The New Yorker. – March 6. – 2017. – P.40–55
8. Presidential Policy Directive/PPD–41 [Електронний ресурс]. – Режим доступу: https://www.whitehouse.gov/the–press–office/2016/07/26/presidential–policy–directive–united–states–cyber–incident
9. Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors… [Електронний ресурс]. – Режим доступу: https://www.documentcloud.org/documents/3766950–NSA–Report–on–Russia–Spearphishing.html#document/p1
10. Secret CIA assessment says Russia was trying to help Trump win White House [Електронний ресурс]. – Режим доступу: https://www.washingtonpost.com/world/national–security/obama–orders–review–of–russian–hacking–during–presidential–campaign/2016/12/09/31d6b300–be2a–11e6–94ac–3d324840106c_story.html?utm_term=.a50061630134
11. Senator Tom Carper requests for information [Електронний ресурс]. – Режим доступу: https://www.carper.senate.gov/public/index.cfm/pressreleases?ID=ECDAEB87–A4C2–4FA2–AA44–EE0F45E9096D
12. US election 2016: Why hackers could tip the result [Електронний ресурс]. – Режим доступу: http://www.independent.co.uk/news/science/us–election–2016–hacking–arizona–illinois–russian–hackers–donald–trump–hillary–clinton–a7217486.html
13. US officially accuses Russia of hacking DNC and interfering with election [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/technology/2016/oct/07/us–russia–dnc–hack–interfering–presidential–election
14. «Активні заходи» СРСР проти США: пролог до гібридної війни». Аналітична доповідь [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/Akt_zah–fc41b.pdf
15. Клинтон обвинила Россию: использует кибератаки против разных организаций в США [Електронний ресурс]. – Режим доступу: http://glavred.info/mir/klinton–obvinila–rossiyu–ispolzuet–kiberataki–protiv–raznyh–organizaciy–v–ssha–390820.html
16. Путин допустил причастность к кибератакам на Западе патриотов РФ [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/486508.php
17. Путин: США – великая держава, а не банановая республика [Електронний ресурс]. – Режим доступу: https://www.gazeta.ru/politics/news/2016/10/27/n_9266717.shtml
18. Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. – К.: НІСД, 2017. – 496 с.

References

1. Background to «Assessing Russian Activities and Intentions in Recent US Elections»: The Analytic Process and Cyber Incident Attribution [Elektronnyi resurs]. – Rezhym dostupu: https://www.dni.gov/files/documents/ICA_2017_01.pdf
2. Bears in the Midst: Intrusion into the Democratic National Committee [Elektronnyi resurs]. – Rezhym dostupu: https://www.crowdstrike.com/blog/bears–midst–intrusion–democratic–national–committee/
3. British spies were first to spot Trump team's links with Russia [Elektronnyi resurs]. – Rezhym dostupu: https://www.theguardian.com/uk–news/2017/apr/13/british–spies–first–to–spot–trump–team–links–russia
4. Cyber researchers confirm Russian government hack of Democratic National Committee [Elektronnyi resurs]. – Rezhym dostupu: https://www.washingtonpost.com/world/national–security/cyber–researchers–confirm–russian–government–hack–of–democratic–national–committee/2016/06/20/e7375bc0–3719–11e6–9ccd–d6005beac8b3_story.html?utm_term=.3946064d9257
5. Grizzly steppe – Russian Malicious Cyber Activity [Elektronnyi resurs]. – Rezhym dostupu: https://www.us–cert.gov/sites/default/files/publications/JAR_16–20296A_GRIZZLY%20STEPPE–2016–1229.pdf
6. Manfred R. Hamm. How Moscow Meddles in the West's Elections [Elektronnyi resurs]. – Rezhym dostupu: http://s3.amazonaws.com/thf_media/1984/pdf/ bg369.pdf
7. Osnos E., Remnick D., Yaffa J. Active measures: What lay behind Russia's interference in the 2016 election—and what lies ahead? // The New Yorker. – March 6. – 2017. – P.40–55
8. Presidential Policy Directive/PPD–41 [Elektronnyj resurs]. – Rezhym dostupu: https://www.whitehouse.gov/the–press–office/2016/07/26/presidential–policy–directive–united–states–cyber–incident
9. Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors… [Elektronnyi resurs]. – Rezhym dostupu: https://www.documentcloud.org/documents/3766950–NSA–Report–on–Russia–Spearphishing.html#document/p1
10. Secret CIA assessment says Russia was trying to help Trump win White House [Elektronnyi resurs]. – Rezhym dostupu: https://www.washingtonpost.com/world/national–security/obama–orders–review–of–russian–hacking–during–presidential–campaign/2016/12/09/31d6b300–be2a–11e6–94ac–3d324840106c_story.html?utm_term=.a50061630134
11. Senator Tom Carper requests for information [Elektronnyi resurs]. – Rezhym dostupu: https://www.carper.senate.gov/public/index.cfm/pressreleases?ID=ECDAEB87–A4C2–4FA2–AA44–EE0F45E9096D
12. US election 2016: Why hackers could tip the result [Elektronnyi resurs]. – Rezhym dostupu: http://www.independent.co.uk/news/science/us–election–2016–hacking–arizona–illinois–russian–hackers–donald–trump–hillary–clinton–a7217486.html
13. US officially accuses Russia of hacking DNC and interfering with election [Elektronnyj resurs]. – Rezhym dostupu: https://www.theguardian.com/technology/2016/oct/07/us–russia–dnc–hack–interfering–presidential–election
14. «Aktyvni zakhody» SRSR proty SShA: proloh do hibrydnoi viiny». Analitychna dopovid [Elektronnyi resurs]. – Rezhym dostupu: http://www.niss.gov.ua/content/articles/files/Akt_zah–fc41b.pdf
15. Klinton obvinila Rossiju: ispol'zuet kiberataki protiv raznyh organizacij v SShA [Elektronnyi resurs]. – Rezhym dostupu: http://glavred.info/mir/klinton–obvinila–rossiyu–ispolzuet–kiberataki–protiv–raznyh–organizaciy–v–ssha–390820.html
16. Putin dopustil prichastnost' k kiberatakam na Zapade patriotov RF [Elektronnyi resurs]. – Rezhym dostupu: http://www.securitylab.ru/news/486508.php
17. Putin: SShA – velikaja derzhava, a ne bananovaja respublika [Elektronnyi resurs]. – Rezhym dostupu: https://www.gazeta.ru/politics/news/2016/10/27/n_9266717.shtml
18. Svitova gibridna viyna: ukrainskiy front: monografiya / za zag. red. V. P. Gorbulina. – K.: NISD, 2017. – 496 s.

Dubov D. V., *Doctor of Political Sciences, Senior Researcher Head of the Department of Information Security and Development of the information society, National Institute for Strategic Studies (Ukraine, Kyiv), shamus123@ukr.net*

Dubova S. V., *Phd in history science, educator academic department information, library and archive business, Kyiv National University of Culture and Arts (Ukraine, Kyiv), sdubova@ukr.net*

«Social cyberataks» as a tool of chaotizing political processes (on the example of the electoral and post– electoral period in the USA in 2016–2017)

Today, cyberattacks are not only a tool for damage by espionage or sabotage, but also a way to influence to political processes in other countries. In fact, cyberspace is becoming another field of struggle used by the Russian Federation to implement a new form of «active measures» – activities aimed to changing the political agenda of a particular country and changing the direction (or political decision) of its leaders. For this, are used «social cyberattacks» whose influence at the socio–political or social dimension, the influence of which is provided through interference in the electoral process. It was on such cyberattacks that the emphasis was laid in the process of Russia's interference in the elections in the USA in 2016 and further chaos of the political process in 2017. Thus, the article is devoted to the study of «social cyberattacks» as a tool for chaotizing political processes (on the example of the electoral and post–election period in the USA in 2016–2017).

It is noted that the chaotic process began with the leakage of 20,000 letters from the United States Democratic Party, the hacking of the internal computer network of the Democratic Party and the use of these data to attack Clinton. Behind the attacks were hackers (two main groups – «Fancy Bear» and «Cozy Bear») associated with the GRU Generalnogo Shtaba of Russian Federation. In addition, Russian's hackers tried to hack into the database of American voters and a American vendors, how designed and develop software for the conduct of electronic elections. The purpose of the actions of destructive cyber–influence was not to directly discredit the election, but to compromise and chaotic the political process as such. This goal, in general, was achieved, since the new leadership of the state was compromised already at the beginning of its cadence. Thanks to cyberattacks, it was possible to destabilize the functioning of the political system of the country with significant political traditions, well–practiced practices of transferring power and well–functioning democratic institutions. In the future, the social component of cyber attacks will only increase.

Keywords: *cyber attacks, election, USA, chaotizing. political processes, Russia.*

* * *

УДК 329.12(436)(045)

Парлюк В. І.,
старший викладач кафедри філософії та соціології,
Маріупольський державний університет
(Україна, Маріуполь), parlykvladislav@gmail.com

Ліберальний напрямок в партійній системі сучасної Австрії

Розглядається положення ліберальних партій в політичній системі сучасної Австрії, електоральні вподобання щодо ліберальних партій, соціальна структура виборців та членів партій. Аналізуються суттєві особливості формування і розвитку лібералізму в Австрії, організаційна структура, програмні засади та офіційні позиції ліберальних партій. Наводяться актуальні фактологічні та статистичні дані, що відображають стан проблеми. Мета даної статті визначити місце ліберальних партій Австрії в партійній системі країни. Підкреслюється важливість і необхідність позитивної перспективи існування ліберальної ідеології в Австрії.

Ключові слова: *партійна система, лібералізм, ліберальні партії та рухи сучасної Австрії, програмні засади, офіційні позиції, вибори, електоральна підтримка.*

Особливості формування і розвитку ліберального напрямку в Австрії сягають своїм корінням ще в імперію Габсбургів. 60–70 рр. XIX ст. увійшли в історію Австрії як ліберальна ера. У ці роки ліберали займали в австрійському Рейхстазі керівні позиції. Однак, поступовий перехід партійної системи до сучасного зразку, заснованому на створенні професійної системи бюрократичного керівництва партійних організацій, представляв проблему для традиційних ліберальних, а також консервативних партій, які прагнули трансформуватися в масові або народні партії, щоб вижити в нових умовах. Політичні партії, що виникли із національних ліберальних традицій, піддаються процесу фрагментації, і їх спроби пристосуватися до постійно змінюваних політичних реалій в основному не увінчалися успіхом. Результатом цих процесів стала ідеологічна дифузія, безперервна втрата ліберальної ідентичності, неоднозначність сформульованих лібералізмом цілей, що призвело до спаду популярності ліберального руху к кінцю 70–х рр. XIX ст. Тому, з початку XX ст. з точки зору партійної політики стало правильніше говорити про «спадкоємців лібералізму», а не просто про «лібералів» [18].

Як і в Першій республіці, так і протягом тривалого часу у Другій республіці, відсутність явно ліберальної політичної партії загрожувало ідеологічно, політично і негативно впливало на австрійський лібералізм.

Причинами «запізнення» політичного лібералізму в Австрії після Другої світової війни можна назвати:

– вигнання і знищення австрійських євреїв (основного суспільного прошарку лібералізму) націонал–соціалістами;

– дві основні політичні партії (Австрійська народна партія (АНП) і Соціал–демократична партія Австрії (СПА)) в своїй діяльності спиралися на традиційне адміністративне і соціально–державне регулювання взаємовідносин між суспільством і державою, що призвело до консенсусного прийняття рішень в предпарламентскому просторі і не дало можливості появи нового ліберального руху;

– австрійський ліберальний рух, починаючи з 90–х рр. XIX ст. знаходився в стані абсолютної роздробленості, створюючи доморощені політичні програми без зв'язку з лібералами інших країн. Саме тому ліберальний рух не мав можливості сформувати і модернізувати адекватну поточній ситуації програму дій. Інші ж партії, приймаючи деякі ліберальні цінності і інструменти, мали можливість впливати на настрої населення, що в кінцевому підсумку значно скорочувало електоральну базу лібералів [9, с. 23].

Всього через чотири роки після краху Третього Рейху і, пов'язаним з цим процесом денацифікації, австрійські націонал–ліберали знову проявляють своє цілком незалежне політичне обличчя. 26 березня 1949 р. зальцбурзькі журналіст Герберт Краус (був лідером партії до 1952 р.) і письменник Віктор Райманн, які під час нацизму були політв'язнями, засновують так звану Асоціацію Незалежних (VDU, ВДУ). Вони відстоювали націонал–ліберальну тезу, що денацифікація, яка не робить різниці між членами НСДАП і фактичними військовими злочинцями може побічно сприяти відродженню нацизму, оскільки торкається прав і свободи багатьох австрійців. Асоціація Незалежних в своїх рядах забезпечила притулок для всіх, хто хотів залишатися в стороні від основних політичних течій того часу: соціалістів і християнських демократів. Членами ВДУ стали не тільки прибічники вільного ринку, ліберали, народники, а й колишні нацисти і німецькі націоналісти, тобто всі, хто не бажав приєднатися до однієї з двох основних партій [1, с. 4]. Слід зазначити, що ВДУ підтримала соціал–демократична партія, так як соціалісти прагнули розколоти правий табір і послабити своїх головних супротивників – АНП [3]. У 1949 р. на національних