державних рішень, робить діяльність державних органів відкритою та прозорою. За останні декілька років в Україні було проведено низку заходів для впровадження та забезпечення ефективного функціонування електронного урядування, більшість державних послуг переведені в онлайн-режим, зроблено крок до впровадження електронного документообігу, продовжують розвиватися електронні портали органів виконавчої влади на різних рівнях електронного урядування. Для покращення теперішньої ситуації необхідно провести заходи щодо погодження нормативно-правових актів, створення навчальних програм та систем, підвищення гарантії захисту персональних даних громадян, створити ефективну систему зворотного зв'язку громадян з державою для покращення ефективності та оперативності прийнятих рішень і діяльності органів державної влади.

Список використаних джерел

1. Сороко В. М. Діяльність публічної адміністрації з надання послуг українському суспільству : монографія / В. М. Сороко, А. В. Вишневський, О. Г. Рогожин ; за ред. Ю. О. Привалова. – Київ : НАДУ, 2007. – 180 с.
2. World Development Report 2016: Digital Dividends. Режим доступа: http://www.worldbank.org/ en/publication/wdr2016. Дата обращения: 02.04.2019.
3. Бєляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Монографія. Київ: КВІЦ, 2008. 576 с.

УДК 32.019.5:004.5(043.2)

Дубель М.В., доктор філософії,
асистент кафедри політології та державного управління

ЗНАЧЕННЯ ДОТРИМАННЯ ПРАВИЛ ЦИФРОВОЇ ГІГІЄНИ ДЛЯ ПОЛІТИЧНОЇ ДІЯЛЬНОСТІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. Питання підтримки цифрової гігієни у сучасному світі є вкрай важливим. Недотримання звичайних правил безпечного використання мережі Інтернет може нести загрозу не лише індивіду, а його оточенню – родині, друзям, колегам по роботі. Особливе значення виконання правил цифрової гігієни у політичній діяльності, тому що наслідки помилок діячів цього напрямку можуть нести загрозу як політичної сили, так і для громадян держави загалом. Отже, саме це робить дослідження **актуальним**.

Аналіз останніх досліджень за даною тематикою. Питання значення цифрової гігієни для функціювання політичних процесів розглядали такі вітчизняні вчені, як М.А. Польовий, Т.В. Бабенко, Ю. Калюжна. Проте, можна підкреслити, що в умовах 2022 року, коли значна частина подій відбувається

в рамках цифрового інформаційного простору, тематика потребує подальшого дослідження.

Мета дослідження – довести значення дотримання цифрової гігієни у політичній діяльності на прикладі розгляду ситуації з витоком інформації Демократичної партії США у 2016 році.

Викладення основного матеріалу. Перш за все потрібно дати характеристику ситуації, що відбулася у 2016 році. Витік електронної пошти Національного комітету Демократичної партії являє собою збірку електронних листів, що були вкрадені одним або декількома хакерами, які діяли під псевдонімом «Guccifer 2.0». Ці електронні листи згодом були передані DCLeaks у червні та липні 2016 р. та WikiLeaks 22 липня 2016 р., незадовго до Національного з'їзду Демократичної партії 2016 р. [1]. До цієї колекції увійшли 19252 електронних листів і 8034 прикріплених файлів від Національного комітету Демократичної партії, керівного органу Демократичної партії США. Витік включає електронні листи від семи ключових співробітників Національного комітету Демократичної партії та датується періодом із січня 2015 року по травень 2016 року. 6 листопада 2016 року WikiLeaks випустив другу партію електронних листів Національного комітету Демократичної партії, додавши до своєї колекції 8263 електронних листів [2].

Електронна пошта, що просочилася Wikileaks, розкрила інформацію про взаємодію Національного комітету Демократичної партії зі ЗМІ, компанії Хілларі Клінтон і Берні Сандерс та фінансові пожертвування. Цей злив також включає особисту інформацію про спонсорів Демократичної партії, включаючи кредитну картку та номери соціального страхування, які можуть полегшити крадіжку особистих даних. Раніше, наприкінці червня 2016 року, Guccifer 2.0 доручив журналістам відвідати веб-сайт DCLeaks, щоб знайти електронні листи, вкрадені у демократів. З розкриттям WikiLeaks додаткових вкрадених листів, починаючи з 22 липня 2016 року, на DCLeaks було опубліковано понад 150 000 вкрадених листів з особистих адрес Gmail або з електронної пошти Національного комітету Демократичної партії, які були пов'язані з президентською кампанією Хілларі Клінтон. 12 серпня 2016 року DCLeaks опублікував інформацію про більш ніж 200 депутатів-демократів, включаючи їхні особисті номери мобільних телефонів. Численні розіграші, які Хілларі Клінтон отримала в результаті цього розкриття, поряд із втратою захисту електронної пошти її кампанії, серйозно підірвали її кампанію, яка змінила свою контактну інформацію 7 жовтня 2016 року, зателефонувавши кожному особисто.

Дві американські компанії, що займаються питаннями інтернет-безпеки, які незалежно один від одного вивчили злом, дійшли висновку, що до нього причетні щонайменше дві групи хакерів. Одна з них, Cozy Bear ("Затишний ведмідь"), мала доступ до серверів комітету з літа 2015 року, про що свідчать дані компанії CrowdStrike, яка проводила розслідування на прохання

Національного комітету Демократичної партії. Торік ці хакери атакували сервери Білого дому, Держдепартаменту та Комітету начальників штабів озброєних сил США [3].

Друга група хакерів, Fancy Bear ("Модний ведмідь"), що діяла незалежно від попередньої, зламала сервери Національного комітету Демократичної партії у квітні 2016 року, встановили в CrowdStrike. Їй також приписують кібератаку на комп'ютерні мережі німецького бундестагу у травні 2015 року та зламування мереж французького телеканалу TV5Monde у квітні того ж року.

Розслідування фірми SecureWorks, підрозділи з кібербезпеки корпорації Dell, показало, що зламування пошти функціонерів Національного комітету Демократичної партії - справа рук хакерської групи TG-4127, яка також зламала домен передвиборчого штабу Хілларі Клінтон hillaryclinton.com, отримавши доступ до листування його співробітників [4]. Атака на Національного комітету Демократичної партії та співробітників передвиборчого штабу, за даними SecureWorks, відбувалася з березня до травня 2016 року.

З точку зору цифрової гігієни потрібно дати роз’яснення технічній стороні цієї ситуації. Проаналізувавши методи роботи хакерів, фахівці SecureWorks дійшли висновку, що TG-4127 і Fancy Bear - та сама група осіб. Зважаючи на все, вони використовували одну і ту ж шкідливу програму та інфраструктуру, щоб отримати доступ до листування Національного комітету Демократичної партії, пояснив Том Фінні, спеціаліст з безпеки в підрозділі SecureWorks по боротьбі з погрозами: "Тобто ці суб'єкти, мабуть, повністю збігаються" [5].

Атаку з боку цих хакерів зазнали електронні скриньки співробітників Національного комітету Демократичної партії та передвиборчого штабу Хілларі Клінтон, створені на поштовому сервісі Google. Щоб отримати доступ до їхньої пошти, зловмисники надсилали їм електронні листи, що містять посилання на підроблений сайт, зовні абсолютно ідентичний веб-сторінці для входу до пошти Gmail.

При цьому ім'я користувача у полі було введено автоматично. Жертві залишалося лише ввести пароль, щоб хакери отримали доступ до її листування. Відповідно, хакери Coz yBear, за даними CrowdStrike, розсилали жертвам посилання на заражений файл, що впроваджує вірус у комп'ютерну систему [4].

Ця ситуація, звісно, мала негативний вплив на Демократичну партію США. Після публікації листування Національного комітету Демократичної партії на ресурсі WikiLeaks голова комітету Деббі Вассерман Шульц пішла у відставку. Згодом, на президентських виборах, що відбулися у листопаді 2016 року, переміг Дональд Трамп. Потрібно розуміти, що не лише цей витік конфіденційної інформації призвів до поразки представника Демократичної партії, але точно не призвів до покращення позиції перед виборами.

Висновки. Отже, на основі розгляду ситуації з витоком інформації Демократичної партії США у 2016 році можна зрозуміти наскільки негативними можуть бути наслідки невиконання правил цифрової гігієни. На жаль, ситуації з фішинговими листами у політичній діяльності стає лише більше, особливо через російських хакерів. Саме тому дотримання основ цифрової гігієни повинно бути обов'язковим серед користувачів, особливо, якщо вони мають відношення до політичної діяльності.

Список використаних джерел

1. *WikiLeaks releases thousands of documents about Clinton and internal deliberations. URL: https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/*
2. *Why it's entirely predictable that Hillary Clinton's emails are back in the news. URL: https://www.washingtonpost.com/news/monkey-cage/wp/2016/11/01/why-its-entirely-predictable-that-hillary-clintons-emails-are-back-in-the-news/*
3. *CrowdStrike's work with the Democratic National Committee: Setting the record straight. URL: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/*
4. *Russian Threat Group Targets Clinton Campaign. URL: https://www.secureworks.com/blog/russian-threat-group-targets-clinton-campaign*
5. *Russian Hacks Show Cybersecurity Limits. URL: https://businessday.ng/technology/article/russian-hacks-show-cybersecurity-limits/*

УДК 303.4:330.341

Зелінська Ю.С., аспірант
Прямухіна Н. В., д.е.н., доцент,
доцент кафедри політології та державного управління

ПЕРЕВАГИ ТА НЕДОЛІКИ ЕМЕРДЖЕНТНИХ СТРАТЕГІЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Перед керівниками та власниками підприємств в умовах високої непередбачуваності змін різноманітних процесів у ринковому середовищі, постає проблема способів зміцнення своїх конкурентних переваг. Для підвищення конкурентоспроможності, підприємства можуть використовувати стратегічне управління, за допомогою якого досягають цілей, шляхом розробки та реалізації різноманітних стратегій.

Намагаючись набути та утримати конкурентні переваги, менеджери підприємств розробляють, приймають та реалізують стратегічні рішення,