

Використання персональних даних виборців під час парламентських виборів в Україні 2019 року: дослідження про цифровий вплив поза межами дезінформації

ТЕТЯНА БОГДАНОВА

стипендіатка Празького центру громадянського суспільства-2020



Липень 2020 року

Подяка

Цей звіт підготовлено за допомогою представників українських та міжнародних організацій громадянського суспільства та за щедрої підтримки Празького центру громадянського суспільства. Погляди, висловлені цій публікації, належать авторці та фахівцям, імена яких наведено нижче, а отже, не обов'язково відображають позицію Празького центру громадянського суспільства або інших організацій.

Авторка: Тетяна Богданова, стипендіатка [Празького центру громадянського суспільства](#) 2020 року, Прага, Чеська Республіка

Юридична радниця: Віта Володовська, керівниця правового напрямку, [Лабораторія цифрової безпеки](#), Україна

Аналіз даних на Facebook: Роберт Лорян, аналітик даних, [Громадянська мережа "ОПОРА"](#), Україна

Дослідження цифрової безпеки: Вадим Гудима, спеціаліст із цифрової безпеки, [Лабораторія цифрової безпеки](#), Україна

Загальний супровід: Варун Башьякарла (Varoon Bashyakarla), аналітик даних, [Tactical Technology Collective](#), Берлін, Німеччина

ЗМІСТ

1. Вступ: мета, предмет дослідження, методологія	4
2. Виборчий цикл 2019: передумови й виклики	5
2.1. Дезінформація, кібератаки та занепокоєння щодо іноземного втручання у вибори 2019 року	5
2.2. Президентські вибори 2019 року та початок використання таргетованої політичної агітації онлайн	5
2.3. Нові правила Facebook щодо виборів	6
2.4. Одночасне застосування легітимних і сумнівних онлайн-практик агітації на президентських виборах	7
3. Парламентські вибори 2019 року	7
3.1. Методи й інструменти проведення виборчої кампанії онлайн: огляд	7
3.2. Політична реклама у Facebook протягом парламентських виборів	12
3.3. Інші питання, що стосуються цифрової агітації	14
4. Онлайн-агітація і збір даних п'ятьма парламентськими партіями	14
4.1. Нормативно-правова база	14
4.2. Веб-сайти	16
4.2.1. Безпека веб-сайтів	27
4.3. Інші методи збору даних в рамках цифрової агітації: Facebook, Google-форми, електронні розсилки, петиції тощо	31
4.4. Месенджери і чат-боти	40
5. Інші джерела персональних даних громадян	41
5.1. Державний реєстр виборців	42
5.2. Витоки інформації, злами та безпекові питання	43
5.3. Напівлегальні і нелегальні джерела	43
5.4. Дані споживачів	46
5.5. Ймовірні джерела даних виборців в політичній агітації 2019 року	46
6. Міркування щодо володіння та обміну даними перед та після виборів	47
6.1. Партійні проекти	47
6.2. Державні установи та народні обранці	48
7. Висновки та рекомендації	50

1. Вступ: мета, предмет дослідження, методологія

2016 рік став вагомим в історії політичних кампаній, оскільки охопив президентські вибори в США, референдум щодо виходу Об'єднаного Королівства з ЄС (Брекзит), а також викликані ними викриття, які спровокували світове обговорення ролі соціальних мереж у виборах та значущості використання персональних даних виборців під час цифрових виборчих кампаній (агітації). Україна мала достатньо часу перед президентськими та парламентськими виборами 2019 року для того, щоб врахувати наслідки цих подій та оновити своє законодавство нормами про цифрову виборчу агітацію. Втім, жодних змін у відповідності до хвилі останніх викликів, пов'язаних з новітніми технологіями, ні до чинного, ні до новоприйнятого виборчого законодавства внесено не було.

Хоча декілька організацій громадянського суспільства дослідили та опублікували детальні доповіді щодо політичної агітації онлайн у 2019 році, жодних досліджень стосовно застосування персональних даних виборців під час виборчої кампанії, а також питань, які виникають на перетині приватності та цифрової агітації, проведено не було. **Мета цього дослідження полягає в тому, аби заповнити ці лакуни шляхом аналізу ставлення п'яти партій, які було обрано до парламенту в результаті парламентських виборів 2019: “Слуга народу”, “Європейська солідарність”, “Батьківщина”, “Опозиційна платформа – За життя” та “Голос”, до персональних даних виборців.**

Зокрема, у цій доповіді ми звертаємо увагу на методи збору інформації онлайн, якими користувалися ці політичні сили під час парламентської виборчої кампанії на своїх офіційних веб-сайтах та сторінках в соціальних мережах, включаючи популярні месенджер-платформи. Ми розглядаємо цю практику з огляду на чинне законодавство, партійні заяви про те, яким чином вони збирали та обробляли персональні дані (наприклад, у політиках конфіденційності на своїх веб-сайтах), а також методи та інструменти цифрової агітації, які застосовувалися політичними суб'єктами на виборах 2019 року. З метою розширення масштабу застосування отриманих матеріалів ми описуємо загальний стан безпеки персональних даних громадян та аналізуємо декілька інцидентів, що є важливими для розуміння сучасного дискурсу питань приватності в Україні. У ході дослідження виборчих кампаній через соціальні медіа, нам особливо стали у пригоді дані про діяльність у Facebook та про платну політичну рекламу партій та їхніх кандидатів, зібрані [Громадянською мережею “ОПОРА”](#) в період з 2019 до 2020 року. Ми також користуємося інформацією, отриманою з публікацій у медіа, доповідей [організацій-спостерігачів](#) та інтерв'ю з фахівцями, які мають широкий досвід роботи з виборчою проблематикою та цифровими політичними кампаніями в Україні.

Однак, предмет цього дослідження доволі обмежений через те, що ми проводили здебільшого зовнішній огляд цифрової діяльності політичних партій. Наприклад, ми не мали внутрішнього доступу до ІТ-технологій або CRM-систем, які партії використовували на виборах, а отже, ми не змогли охопити всю практику збору та обробки даних, а також їх використання під час онлайн-агітації. Наш огляд таргетованої цифрової реклами і залучення виборців значно обмежений даними Facebook, оскільки цією платформою користувалися всі п'ять партій, про які йтиметься в цій публікації, та завдяки їй

можливостям розміщувати мікротаргетовані політичні оголошення і доступом до детальної інформації про активність виборців онлайн.

Для аналізу партійних веб-сайтів та їхньої діяльності в соціальних мережах ми зосереджувалися на офіційних веб-сайтах (у випадках, коли партія користувалася більше ніж одним сайтом, ми розглядали той, який з них найбільше використовувався для взаємодії із виборцями й збору даних протягом виборчої кампанії) та на їхніх офіційних сторінках у Facebook, за винятком, коли допоміжні сторінки проводили платну політичну агітацію від імені партії. Також, з метою проведення змістовного аналізу цифрової діяльності партій під час виборів ми деколи аналізували веб-сайти та сторінки у соціальних мережах з ретроспективної точки зору та із застосуванням Інтернет-архіву. Ми також не систематизували дані стосовно регіональних, афілійованих або індивідуальних сайтів кандидатів та їхньої діяльності в соціальних мережах, тому лише акцентуємо на них в разі, коли це необхідно для отримання повного уявлення про методи цифрової агітації і ставлення до даних виборців з боку певної політичної сили.

2. Виборчий цикл 2019: передумови й виклики

2.1. Дезінформація, кібератаки та занепокоєння щодо іноземного втручання у вибори 2019 року

Існує достатньо доказів того, що російські державні суб'єкти та пов'язані з ними особи проводили дезінформаційні кампанії в Україні щонайменше починаючи з 2014 року. Інститут Інтернету Оксфорду назвав ці кампанії "[найвизначнішим кейсом пропаганди з використанням комп'ютерних технологій](#)" проти країни. Наприклад, у 2016 році український Інтернет-портал Texty.org.ua викрив скоординовану мережу, що складалася із [більше ніж 2 000 облікових записів у Facebook](#), пов'язаних з російською фермою тролів, які протягом 8 місяців вели онлайн-кампанію з метою скинути український уряд.

Дослідження, проведене у 2018 році VoxUkraine, проаналізувало понад [9 мільйонів твітів, пов'язаних з російським «Агентством Інтернет-досліджень»](#), 750 тис. з яких стосувалися України. Така дезінформаційна кампанія спалахнула під час Євромайдану у 2014 році і поступово набирала обертів з окупацією та анексією Криму, досягнувши свого піку на наступний день після падіння літака МН17 на території Східної України.

Цей та інші випадки викликали занепокоєння щодо виборів 2019 року та ймовірності іноземного втручання. Втім, хоча російська дезінформація протягом виборів [залишалася настільки ж масовою, як і раніше](#), а [пов'язані з Росією хакери](#) намагалися підірвати електронну інфраструктуру, [вони не спромоглися поширити свій вплив настільки](#), щоб суттєво вплинути на процес голосування та результати виборів.

2.2. Президентські вибори 2019 року та початок використання таргетованої політичної агітації онлайн

2019 рік став першим роком, коли соціальні мережі здійснювали [значний вплив](#) на політичну агітацію, адже [21,4 мільйони Інтернет-користувачів](#) та [23,5% українців](#) загалом

обрали соціальні мережі основним джерелом новин. Тренд задав Володимир Зеленський, якому вдалося привернути увагу аудиторії, що раніше не цікавилася виборами, але активно користувалася Facebook, Instagram і Telegram. Він змусив використовувати нові “правила гри” і своїх опонентів, включаючи чинного на той час Президента Петра Порошенка, який розширив свою кампанію з Facebook ще й на Instagram і Telegram.

Згідно з Михайлом Федоровим, головним цифровим стратегом Зеленського, а пізніше міністром України з цифрової трансформації, основний акцент їхньої кампанії було зроблено на залученні виборців. Для цього у штабі створили багато спеціальних ініціатив, які по-різному заохочували користувачів брати в них участь. Ще одна особлива тактика Зеленського полягала в розширеному застосуванні мікротаргетингового функціоналу, який пропонують цифрові платформи, зокрема Facebook, для надсилання спеціалізованих повідомлень різним групам.

Як [визнав](#) сам Федоров, у ході виборів цільову аудиторію кампанії було розділено на 32 категорії згідно з віком, статтю, професійними або політичними інтересами та проведено близько 3 200 таргетованих рекламних кампаній. Було також надіслано [21 млн. електронних листів](#), набрано 130 тис. підписників у Telegram каналі та 608 527 волонтерів онлайн, враховуючи 20 тис. спостерігачів за виборами та 10 тис. працівників комісій, які надавали детальні персональні дані, аби отримати ці посади. Команда також використовувала чат-ботів, один з яких допомагав виборцям знайти свої виборчі дільниці на базі даних про їхнє місце проживання.

2.3. Нові правила Facebook щодо виборів

Перед президентськими виборами 2019 року Facebook [оголосив](#) про нововведення, які мали попередити дезінформацію та іноземне втручання шляхом посилення прозорості платної політичної реклами та більш детального аналізу поведінки користувачів. Нові правила вимагали від тих, хто розміщує політичну рекламу, [вказувати свої персональні дані, місце розташування та зазначити, ким оплачена реклама](#), і передавати ці дані на схвалення Facebook. Він також відкрив публічну бібліотеку політичної реклами, яка містила всю політичну та соціальну рекламу, що стосувалася України та демонструвалася з дисклеймером про платну рекламу або без нього і мала політичний контент або контент, пов'язаний з певними політичними питаннями.

Втім, через повільну імплементацію та серйозні прогалини нові прозорі правила були неефективними аж до моменту, коли до першого туру виборів залишалося два тижні. Наприклад, географічні вимоги можна було обійти шляхом “передачі облікового запису в оренду” рекламодавцю, який знаходився за кордоном – практика, про яку Служба Безпеки України [повідомляла](#) ще в січні 2019 року. Окрім цього, проблемний контент, про який повідомляли учасники виборів, [вилучався зі значною затримкою](#), а облікові записи, що багаторазово порушували правила, [мали змогу й надалі](#) розміщувати рекламу.

Врешті-решт, варто зазначити, що інші онлайн-платформи, такі як Twitter або Google, проігнорували введення подібних безпекових заходів, а от на таких платформах, як Youtube, моніторинг політичної реклами практично неможливий.

2.4. Одночасне застосування легітимних і сумнівних онлайн-практик агітації на президентських виборах

У ході аналізу платних політичних оголошень у Facebook українська організація, що спостерігає за виборчим процесом “ОПОРА” та міжнародна організація Demogasy Reporting International виявили [неофіційні сторінки на Facebook](#) пов’язані з [офіційними акаунтами](#) основних кандидатів на виборах, що поширювали хибні та дискредитуючі дані про опонентів.

Окрім цього, спостерігачі [помітили](#) активну діяльність ботів і “фейкових” облікових записів, що використовувалися у ході онлайн-агітації, яких часто ідентифікували і видаляли самі соцмережі. Журналісти, які проводили розслідування, змогли опитати декількох осіб, які керували такими обліковими записами на комерційній основі. Згідно з оцінкою одного з них, протягом виборів 2019 року лише на Facebook було створено понад [200 тис.](#) [“фейкових” облікових записів](#), а вартість однієї такої “операції” варіювалася від 1 тис. до 50 тис. або навіть 100 тис. дол. США в залежності від масштабу.








3. Парламентські вибори 2019 року

3.1. Методи й інструменти проведення виборчої кампанії онлайн: огляд

Коли внаслідок раптового розпуску Парламенту 21 травня 2019 року новообраним Президентом Володимиром Зеленським партії отримали невеликий перепочинок між двома виборчими циклами, вони швидко переорієнтувалися на парламентські вибори, застосовуючи ті самі онлайн-платформи, персонал і методи агітації. Зокрема, партії знову звернулися до Facebook – найпопулярнішої на сьогодні соціальної мережі в країні, що охоплює близько [14 мільйонів користувачів](#). Водночас, партії та кандидати активно використовували Instagram ([11 мільйонів користувачів у 2019 році](#)), Youtube, Twitter, такі месенджери як Viber і Telegram, а також мобільні додатки.

З-поміж інструментів цифрової агітації партії активно користувалися можливостями онлайн-реклами на різних платформах (від Facebook до Instagram, від Youtube до Google). Відповідно до інтерв’ю, проведеним для цього дослідження з одним із цифрових політичних маркетологів, партії активно використовували переваги таких інструментів таргетингу, як [“Lookalike Audiences”](#) та [“Custom Audiences”](#) Facebook, які здатні оцінювати ефективність реклами і активно просувати особливо успішний контент. Враховуючи невеликі розміри аудиторії, що цікавила партії, такі інструменти як A/B тестування не були ефективними і для онлайн-оголошень, і для електронної розсилки. До того ж, не кожна партія застосовувала навіть автоматизовану CRM-систему, виходячи з того, наскільки дорого така системи може коштувати чи наскільки важко адаптувати її до українського ринку.

Підсумкова таблиця отриманих нами даних щодо використання цифрових платформ* п'ятьма партіями для виборчої агітації

Партія	Веб-сайт							Інше
«Слуга народу»	✓	✓	✓	✓		✓	✓	Мобільні додатки
«Європейська Солідарність»	✓	✓	✓	✓	✓		✓	
«Батьківщина»	✓	✓	✓	✓		✓	✓	
«Голос»	✓	✓	✓	✓	✓	✓	✓	
«Опозиційна Платформа – За Життя»	✓	✓	✓					

* Зображення: *Creative Commons*

Партія “Слуга народу” набрала [найбільшу кількість підписників у соціальних медіа](#) (включаючи понад 256 тис. на Facebook станом на день виборів 2019 року¹) і стала третьою за кількістю залучених підписників станом на початок 2020 року. Вона навіть називала себе “[Інтернет-партією](#)”, акцентуючи на тому, що вона активно діє онлайн. Під час виборів їхні SMM-спеціалісти змогли успішно [перевести політику до Instagram і Telegram](#) з тих платформ, до яких українці звикли більше: з Facebook і Twitter. “Слуга Народу” була особливо активною партією у Facebook протягом виборчої кампанії в усьому, що стосувалося залучення аудиторії (цей тренд зберігся з часів президентської кампанії) і посіла третє місце серед п'яти парламентських партій за витратами на політичну рекламу на Facebook. Ця партія також активно використовувала головну сторінку з метою просування своїх акаунтів на різних платформах. Наприклад, партія часто просила користувачів долучитися до їхнього Telegram-каналу, щоб бути в курсі найсвіжіших новин, або використовувати чат-ботів, аби отримувати базові дані про партію (Зображення 1), повідомляти про дезінформацію, або ж про порушення під час виборчого процесу.

¹ Згідно з моніторингом Facebook, проведеним «ОПОРОЮ».



Зображення 1: 20 червня 2019 року, пост партії “Слуга Народу” у Facebook, який оголошує про створення чат-боту-помічника у Telegram, скріншот від 14.03.2020.

Партія також заохочувала прихильників створювати регіональні облікові записи в Facebook і Telegram-канали, на які потім посилалася на головній сторінці, щоб кількість підписників зростала ще більше (багато з яких діяли ще з часів президентської кампанії). Також створювалися веб-сторінки для кандидатів від одномандатних округів. Водночас, партія вела окремий сайт для розвінчання фейків (публікацій у соціальних медіа, що містили неправдиву інформацію про “Слугу Народу”), про які повідомляли прихильники – ініціатива, яку теж було започатковано під час президентської кампанії і яка набрала надвисокої популярності серед користувачів соціальних мереж. Ще однією інновацією, яку впровадила партія “Слуга Народу”, став [мобільний додаток](#)² (доступний для [iOS](#) та [Android](#)), запроваджений для комунікації з виборцями.

“Європейська солідарність” мала на початку 2020 року понад [400 тис. підписників](#) в соціальних мережах (включаючи 303 тис. на Facebook на день виборів у 2019 році³) і входила в трійку лідерів за залученням аудиторії. Вона наслідувала приклад “Слуги Народу” і проводила агітацію на інших платформах, таких як месенджери Telegram і Viber, Twitter, Instagram та Youtube. Оскільки в її рядах були інші відомі особистості, партія також активно використовувала свою сторінку Facebook, щоб взаємодіяти з їхніми сторінками та просувати свої акаунти на інших платформах (Зображення 2). “Солідарність” стала другою за розміром витрат на політичну рекламу в Facebook серед п’яти парламентських партій.

² Веб-сайт не активний.

³ Згідно з моніторингом Facebook, проведеним «ОПОРОЮ».



Зображення 2: 13 червня 2019 року, пост "Європейської солідарності" у Facebook, який містить активні посилання на сторінки інших кандидатів і акаунти партії на інших платформах, скріншот від 17.03.2020.

"Батьківщина", маючи [понад 400 тис. підписників](#) у соціальних медіа на початку 2020 року (включаючи понад 341 тис. підписників на Facebook на день виборів 2019 р.)⁴, також вела активну онлайн-агітацію та посіла четверте місце за витратами на рекламу у Facebook. Партія також закликала своїх прихильників підписатися на її акаунти на інших платформах, зокрема, на Youtube, а також взаємодіяти зі сторінкою їхньої партійної лідерки Юлії Тимошенко.

"Опозиційна платформа – За життя" традиційно була найменш активною в соціальних мережах. Вона веде обліковий запис у Facebook, що мав трохи більше ніж 44 тис. підписників станом на день виборів 2019⁵ року, має скромний Instagram акаунт та посіла останнє місце серед парламентських партій за обсягом витрат на рекламу в Facebook. Це можна пояснити тим, що основний електорат партії складається з виборців старшого віку, які зазвичай менш активні в соціальних мережах. Що ж до взаємодії із користувачами, ОПЗЖ використовувала обліковий запис Facebook здебільшого для того, щоб привести читачів на її партійний веб-сайт (Зображення 3).

⁴ Згідно з моніторингом Facebook, проведеним «ОПОРОЮ».

⁵ Згідно з моніторингом Facebook, проведеним «ОПОРОЮ».



Зображення 3: 6 червня 2019 року, Facebook-пост “Опозиційної платформи – За життя”, в якому вона ділиться публікацією з веб-сайту партії, скріншот від 18.03.2020.

“Голос” – наймолодша партія на українській політичній сцені із [трохи більше ніж 90 тис. підписників](#) (станом на січень 2020 року). Утім, вона посіла одне з перших місць у рейтингу залучення підписників і користувалася більшою кількістю соціальних платформ, ніж інші, включаючи навіть Soundcloud. Партія приділила багато уваги онлайн-агітації і витратила найбільшу суму серед п’яти партій на рекламу у Facebook. Вона також використовувала платформу для того, аби закликати прихильників підписатися на акаунти партії в інших соціальних медіа. До того ж, “Голос” однією з перших [запустила Telegram-бота](#) для взаємодії з виборцями. Свою сторінку у Facebook партія застосовувала і для розвінчання “фейків” (публікацій у соціальних медіа, що містили неправдиві дані про “Голос”) (зображення 4).



Зображення 4: 22 червня 2019 року, публікація “Голосу” на сторінці у Facebook, яка попереджає підписників про неправдиву інформацію про партію, яку поширили в мережі, скріншот від 11.03.2020.

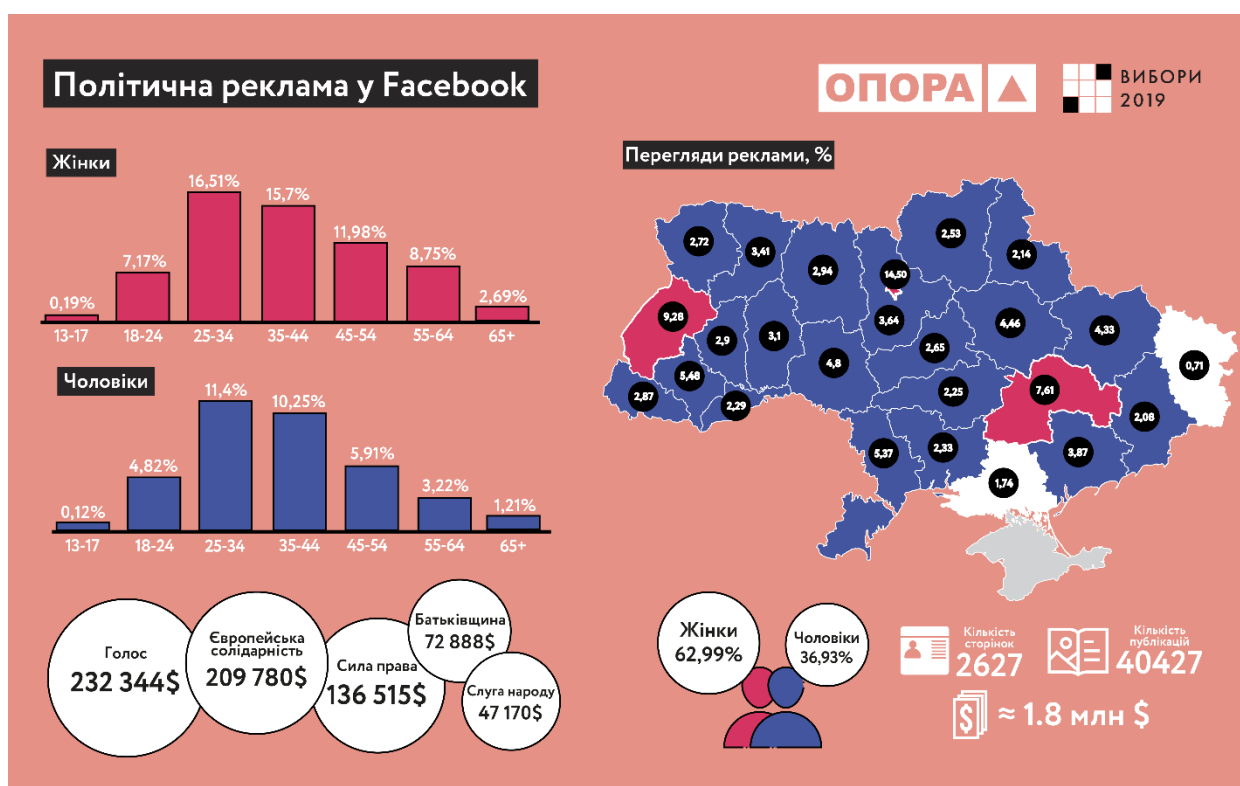
3.2. Політична реклама у Facebook протягом парламентських виборів

Попри те, що, згідно із висновками громадської організації “Чесно”, що [проаналізувала фінансові витрати на виборчі кампанії](#), всі парламентські партії мали схожу структуру фінансових витрат протягом передвиборчої кампанії (найбільша доля ресурсів виділялася на телевізійну рекламу, за нею слідувала зовнішня реклама), деякі політичні сили скористалися наявними правовими прогалинами і не доповіли про свої витрати на онлайн-агітацію.

Отже, за відсутності чіткого правового механізму, за яким кандидати мають звітувати або

за яким регулятори можуть проводити моніторинг витрат на онлайн-рекламу, бібліотека політичної і соціальної реклами Facebook, нещодавно запроваджена в Україні, стала єдиним джерелом, звідки можна було отримати орієнтовну інформацію про витрати політсил на онлайн-агітацію. Жодна інша платформа не забезпечила такого рівня прозорості.

Використовуючи дані Facebook, Громадянська мережа “ОПОРА”, що здійснювала моніторинг виборчої кампанії, встановила, що партії провели [40 427 таргетованих політичних рекламних акцій](#) протягом періоду активної агітації й витратили на них понад 1 800 000 доларів США (Зображення 5). Водночас, перегляд проміжних фінансових партійних звітів виявив значне заниження цифр, що стосуються витрат на онлайн-агітацію, задекларованих учасниками виборів у порівнянні з кількістю проведених рекламних кампаній у Facebook.



Зображення 5: політична реклама на Facebook під час парламентських виборів 2019 року, опублікована 5 найпопулярнішими партіями за рівнем витрат, інфографіка “ОПОРИ”.

Хоча виборче законодавство України, станом на 2019 р., не врегульовувало онлайн-агітацію, воно забороняло кандидатам використовувати власні кошти партій, кандидатів або фінансування з інших джерел, включаючи ініціативу виборців. Отже, третім сторонам було заборонено оплачувати рекламу в соціальних мережах. Втім, за відсутності чітких правових механізмів покарати особу за агітацію в Інтернеті і соціальних мережах через фінансування, незадеклароване у виборчому фонді, неможливо. Як було вказано вище, чи не єдиним способом оцінити витрати партій на цифрову рекламу, а також визначити джерело її фінансування – була бібліотека політичної реклами Facebook.

Згідно з представником руху за прозорість і підзвітність у політиці “Чесно”, лише [три партії](#) на виборах 2019 року задекларували свої витрати таким чином, що цифри орієнтовно

збігалися з даними бібліотеки політичної реклами Facebook.

Деякі партії, такі як “Опозиційна платформа – За життя”, проводили всі свої рекламні кампанії з неофіційної сторінки “Бойко – Прем’єр-міністр” (названої на честь одного з партійних лідерів Юрія Бойка). Реклама на підтримку “Батьківщини” проводилася з фан-сторінки Юлії Тимошенко та з її офіційної сторінки.

3.3. Інші питання, що стосуються цифрової агітації

Як і під час президентських виборів, “ОПОРА” фіксувала [випадки агітації з елементами так званого “чорного піару”](#), опублікованих сторінками, що не були напряму пов’язані з жодною політичною силою. На додаток, коаліція медіа спостерігачів доповідала, що більше половини політичних партій, враховуючи їхніх лідерів, застосовували в своїх публікаціях на Facebook [елементи мови ворожнечі](#), спрямовані на дискредитацію їхніх опонентів на виборах 2019 року.

Нарешті, журналісти зі “Слідство.Інфо”, які проводили детальне розслідування, виявили підпільну ферму ботів, яка пропонувала професійні послуги зі створення сотень “фейкових” акаунтів на Facebook, що потім залишатимуть десятки тисяч “коментарів” на підтримку або ж проти певного кандидата. Журналіст під прикриттям [пропрацював на цій “фермі” протягом декількох тижнів](#) у групі, яка залишила близько 40 тис. коментарів, що коштували учасникам виборів приблизно 20 тис. євро. Хоча використання ботів не заборонене (і взагалі жодним чином не врегульоване) українським виборчим законодавством, незадеклароване фінансування подібних послуг є незаконним.

4. Онлайн-агітація і збір даних п’ятьма парламентськими партіями

4.1. Нормативно-правова база

П’ять партій, які зайняли місце в парламенті у 2019 році: “Слуга народу”, “Опозиційна платформа – За життя”, об’єднання “Батьківщина”, “Голос” і “Європейська солідарність” зверталися до різноманітних методів онлайн-агітацій, щоб привернути увагу виборців.

Наприклад, вони закликали їх підписуватися на електронні розсилки, слідкувати за партійними соціальними сторінками або приєднуватися до груп і каналів у месенджерах, користуватися ботами в месенджерах або встановлювати мобільні додатки. Більшість цих механізмів забезпечували підписників інформацією про партію та її кандидатів, їхню передвиборчу програму та останні новини, а також базову інформацію про голосування. На додаток, деякі партії використовували свої веб-сайти й соціальні медіа, щоб активно залучати нових членів, волонтерів і кандидатів.

Попри активне використання онлайн-інструментів для агітації, ні виборче законодавство, що діяло у 2019 році, ні новоприйнятий Виборчий кодекс не містили регулювання безпекових заходів для захисту персональних даних користувачів чи визнавали цифрову

політичну рекламу однією з офіційних форм агітації.

Втім, закон України «Про захист персональних даних», прийнятий у 2010 році, встановлює обов'язкові умови для всіх аспектів автоматизованої обробки даних. Ці вимоги мають також стосуватися онлайн-збору даних виборців, а також процесів їхньої обробки політичними партіями й кандидатами.

Особливо суттєво прийнятий закон посилив безпеку персональних даних, які стосуються політичних поглядів та членства в політичних партіях (стаття 7).

Таким чином, [норми законодавства](#) вимагають від установ повідомляти Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, які створюють особливий ризик для прав і свобод суб'єктів цих персональних даних (так звані «чутливі дані»).

Це, зокрема, стосується інформації про політичні, релігійні або ідеологічні погляди особи, її членство в політичних партіях та/або організаціях, профспілках, релігійних організаціях, або в публічних організаціях ідеологічної спрямованості. Однак, політичні партії і деякі категорії організацій громадянського суспільства [звільняються від цих вимог](#), у випадку, якщо дані стосуються їхніх членів, які надають їх партії/ОГС за власною волею. Водночас, залишається незрозумілим, як варто ставитися до даних, що надаються особами, які не є членами партії/ОГС (наприклад, волонтерами, прихильниками або іншими виборцями), зібраними політичною партією під час виборів.

Під час написання цього звіту ми подали офіційний запит на надання інформації до Секретаріату Уповноваженого та отримали відповідь про те, що жодна з п'яти парламентських партій не надала таке повідомлення у 2019 році. До того ж, ми не знайшли жодної публічної інформації, яка б підтверджувала факт подання таких повідомлень будь-якою з п'яти партій з моменту вступу цієї норми в дію у 2014 році.

Проте, на основі цих норм та інших регулювань, персональні дані виборців мають опрацьовуватися політичними партіями після того, як суб'єкт даних надасть однозначну згоду на обробку особистої інформації, а партії забезпечать їй належний захист, а також забезпечать те, що ця інформація не буде передана третій стороні без згоди виборця.

Стаття 6 закону «Про захист персональних даних» також встановлює, що обробка даних має проводитися для конкретних і законних цілей за згодою суб'єкта даних. Суб'єкт даних має також мати право відкликати свою згоду на обробку даних або давати згоду на обробку своїх даних відповідно до зміненої цілі.

Згода – фундаментальна основа для електронної обробки персональних даних виборців для політичних кампаній за законом «Про захист персональних даних» – має відповідати таким принципам:

- *Добровільна* – виборець має змогу на власний розсуд вирішувати, яку інформацію він/вона надає;
- *Однозначна* – вимагає, щоб виборець особисто поставив позначку в належному місці або власноруч ввів персональні дані на сайті;

- *Поінформована* – означає, що користувач має отримати зрозумілу і повну інформацію про те, як саме оброблятимуться його/її персональні дані, ким, з якою метою, які методи застосовуватимуться, як цю інформацію використовуватимуть, чи буде вона надана третім сторонам, і якщо так, то кому і з якою метою.
- *Попередня* – обробка персональних даних не може починатися до моменту надання згоди (наприклад, доки користувач не поставить позначку у відповідному полі на веб-сайті).

Стаття 12 встановлює, що користувачу (тобто, суб'єкту персональних даних), має надаватися інформація про те, яка установа збирає його/її дані, склад та зміст зібраних персональних даних, його/її права, визначені цим законом, мету збору персональних даних та осіб, яким передаються його/її персональні дані, у момент збору таких даних.

Стаття 24 зобов'язує тих, хто проводить обробку персональних даних, захищати ці дані від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Це означає, що партії мають застосовувати таке технічне обладнання, яке відповідає б потребам захисту своїх веб-сайтів з метою забезпечення цілісності й захисту даних користувачів.

4.2. Веб-сайти

Всі п'ять партій активно використовували свої веб-сайти для залучення членів, кандидатів та волонтерів – для цього вони просили користувачів зареєструватися онлайн і вказати своє повне ім'я, контактну інформацію, місце проживання й інше. Онлайн-лічильниками було підраховано, що лише на сайтах “Слуги народу” та “Європейської солідарності” перед виборами зареєструвалось **102 тис. осіб**.

Наш аналіз веб-сайтів та акаунтів п'яти парламентських політичних партій у соціальних медіа під час парламентської кампанії 2019 року свідчить, що жодна не дотрималась вимог і принципів отримання поінформованої згоди користувачів, встановлених у законі «Про захист персональних даних», в повному обсязі.

Лише дві партії (“Голос” та “Слуга народу”) пропонували виборцям ознайомитися з політикою конфіденційності, в якій були вказані такі деталі: які саме дані про них будуть отримані і з якою метою, чи будуть вони надаватися третім сторонам, як захищатимуться дані, або які права має суб'єкт даних. Лише три з п'яти партій просили користувачів надати деталізовану згоду на обробку їхніх персональних даних, зібраних шляхом онлайн-реєстрації (“Голос”, “Європейська солідарність” та “Слуга народу”).

Дві партії (“Європейська солідарність” і “Батьківщина”) пропонували користувачам долучитися до їхньої електронної розсилки. “Європейська солідарність” вказала, що надана інформація може використовуватися ще й для іншого, але не зазначаючи, для чого конкретно (хоча партія й пропонувала користувачам дати згоду на “інше”), що суперечить принципу поінформованої згоди. “Батьківщина” використовувала сервіс MailChimp, щоб управляти електронною розсилкою, але ніде не вказувала і не питала згоди користувачів на те, що електронні адреси будуть передані до цього сервісу (тобто, до третьої сторони). “Опозиційна платформа – За життя”, своєю чергою, взагалі не

деталізувала, як використовуватиметься інформація, надана користувачами, які натискали на загальну кнопку “Приєднатися” на партійному веб-сайті.

Чотири з п’яти партій (за винятком “Європейської солідарності”) також використовували різноманітні аналітичні сервіси, здатні відстежувати активність особи в мережі та надсилати дані третім сторонам – наприклад, Google Analytics or HotJar. Всі п’ять застосовували cookies і трекари, встановлені соціальними мережами з рекламними цілями (включаючи Facebook, Twitter і Youtube). Лише дві партії, веб-сайти яких мали політику конфіденційності, намагалися інформувати користувачів про такі деталі, але й вони не питали їхньої згоди на використання cookies (навіть тих, що не були життєво важливими для роботи сайту), і не пропонували винятків з переліку опції використання персональних даних іншими платформами для маркетингових чи рекламних цілей. Жоден із веб-сайтів не попереджав користувачів про те, що вони надають персональні дані з моменту переходу на їхній сайт.

Простий огляд веб-сайтів також виявив деякі безпекові питання, які можна розглядати як порушення статті 24, що забезпечує захист персональних даних. Наприклад, “Європейська солідарність” встановила на своєму веб-сайті незашифрований канал зв’язку із третьою стороною – хостингом їхньої фотогалереї, а веб-сторінка “Опозиційної платформи – За життя” використовувала звичайний HTTP протокол, що робить усі дані, надані на сайті користувачами, доступними в простому текстовому форматі для будь-кого, хто стежитиме за з’єднанням.

Підсумкова таблиця наших висновків стосовно партійних веб-сайтів⁶

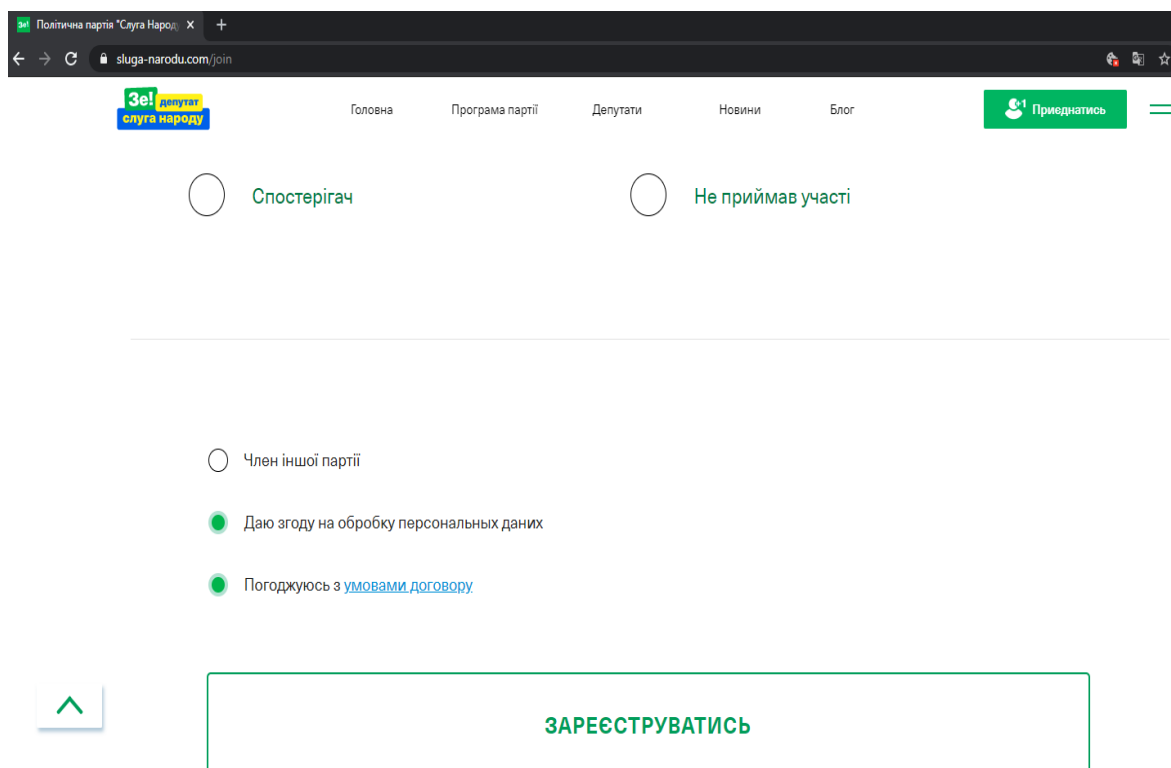
Партія	”Слуга народу”	”Європейська солідарність”	”Батьківщина”	”Опозиційна платформа – За життя”	”Голос”
URL	https://sluga.narodu.com/	https://eurosolidarity.org/	https://ba.org.ua/	http://zagittya.com.ua/	https://golos.zmin.org/
Пропонує користувачам надати персональні дані (ім’я, адресу, телефон)	✓	✓	✓	✓	✓
Має політику конфіденційності	✓				✓
Просить дати згоду на збір/обробку персональних даних	✓	✓			✓
Використовує Google Analytics	✓		✓	✓	✓

⁶ Виявлення трекарів і cookies проводилося за допомогою [Ghostery](#), [Cookiebot](#), функцією перегляду cookies на Chrome та ручному перегляді коду веб-сайтів.

Використовує трекари Facebook або інших соціальних медіа	✓	✓	✓	✓	✓
Використовує інші cookies	✓	✓	✓	✓	✓
Потенційні безпекові проблеми ⁷		✓	✓	✓	✓

Більш детальний аналіз веб-сайту кожної партії наведено нижче.

Партія “Слуга народу” була однією з двох парламентських партій (разом із “Голосом”), які пропонували своїм прихильникам детальну політику конфіденційності на своїх веб-сайтах та єдиною з п’яти, хто просив користувачів прийняти політику і додатково надати згоду на обробку персональних даних в окремому полі. Обидві опції залишалися активними як мінімум на початок 2020 року (Зображення 6).



Зображення 6: розділ “Приєднатись” на веб-сайті “Слуги народу”, що запрошує користувачів долучитися до партії, скріншот від 24.02.2020.

Партія набирала волонтерів, членів і кандидатів онлайн. У розділі “Приєднатись” користувачам пропонували надати доволі розширену інформацію про себе: повне ім’я,

⁷ Було проведено неповний безпековий аналіз сайтів, оскільки повний аналіз вимагає доступу зсередини.

номер телефону, електронну адресу і повну адресу місця реєстрації (Зображення 7-8). У деяких випадках [збиралася](#) додаткова персональна інформація (наприклад, від добровольців, які реєструвалися для спостереження за виборами або роботі у виборчих комісіях). Згідно з лічильником на партійному веб-сайті, станом на 16 липня 2019 року реєстраційну форму заповнили **50 665 осіб**.

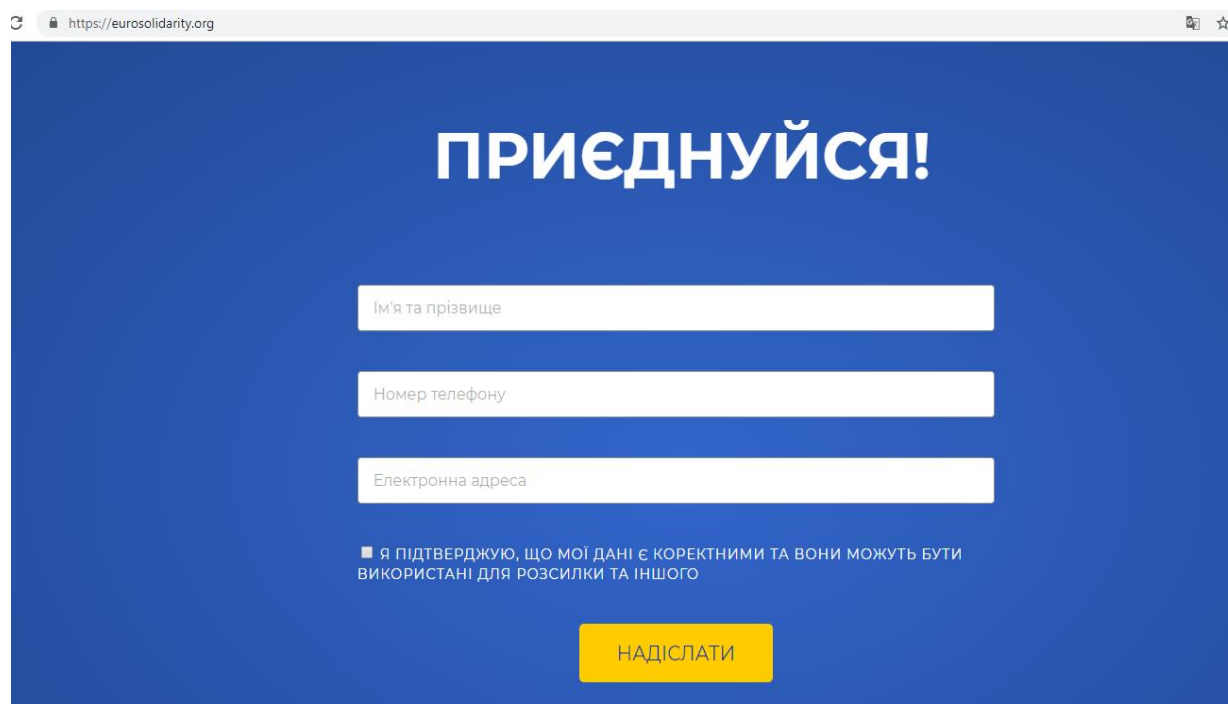
Зображення 7: веб-сайт “Слуги народу”, поля для заповнення персональних даних в розділі “Приєднатись”, скріншот від 16.07.2019.

Посегнутти кандидатам')."/>

Зображення 8: веб-сайт “Слуги народу”, поля для заповнення персональних даних в розділі “Приєднатись” (продовження), скріншот від 16.07.2019.

Політика конфіденційності партії “Слуга народу” ([версія від 25 травня 2019 року](#)) перелічувала шляхи і типи даних, які збирали про користувачів (тобто інформація, надана ними під час реєстрації, зібрана про відвідувачів через Google Analytics, а також дані, отримані завдяки cookies), мету збору та випадки, в яких доступ до даних може отримати третя сторона. Вона також роз’яснювала права користувачів стосовно їхніх персональних даних, наприклад, право доступу до даних, зібраних про них партією. Хоча в політиці конфіденційності зазначено, що інформацію, отриману з cookies, “не розкривають третім сторонам, ці дані не будуть передані третім сторонам неправомірним чином”, веб-сайт надавав можливість встановлювати сторонні cookies, які відстежують діяльність відвідувачів в мережі, та ділитися цими даними з Facebook. Як вже було зазначено вище, користувачів не інформували про це одразу після входу на веб-сайт, а лише на сторінці, де була описана політика конфіденційності.

Як було виявлено, “Європейська солідарність” вела два веб-сайти протягом виборчої кампанії, й лише один з них був вказаний на їхній офіційній Facebook-сторінці, а інший, при спробі отримати доступ до його архівної версії, перенаправляв нас на “головний” сайт. Отже, ми аналізували лише цей основний сайт, через який партія також збирала інформацію про виборців. Так, на цьому сайті “Солідарність” пропонувала лише одну реєстраційну форму з полями для повного імені, номеру телефону й електронної адреси (див. Зображення 9). Після відправлення форми користувачі мали відмітити поле на підтвердження їхнього розуміння про те, що інформація, яку вони надали, є вірною і може бути використана “для електронної розсилки та іншого”. Пояснення цього “іншого” або будь-якої іншої деталізації використання персональних даних виборців ніде на сайті ми не знайшли. Це порушує принципи згоди, наведені вище. Аналіз також засвідчив, що веб-сайт не використовував Google Analytics, але дозволяв використовувати маркетингові cookies з Twitter. Згідно з партійним лічильником, станом на день виборів 21 липня 2019 року форму “Приєднуйся!” заповнили **52 627** користувачів.



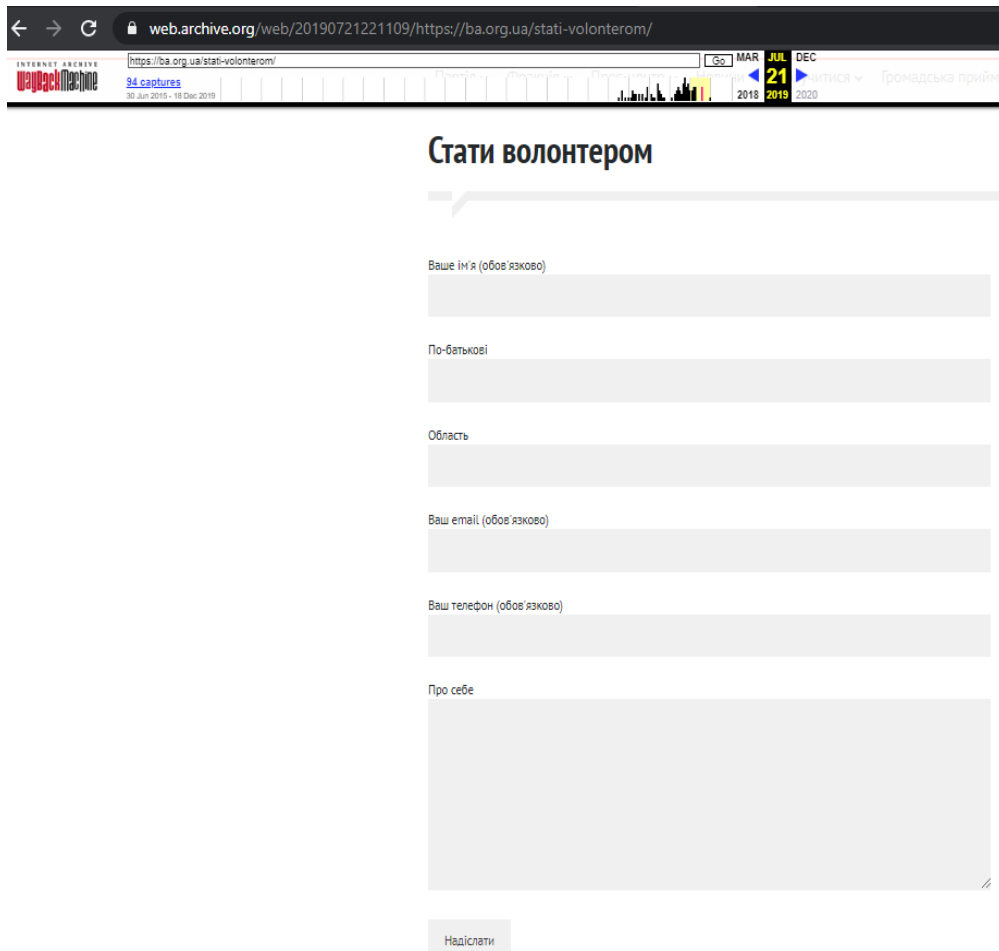
https://eurosolidarity.org

ПРИЄДНУЙСЯ!

Я ПІДТВЕРДЖУЮ, ЩО МОЇ ДАНІ Є КОРЕКТНИМИ ТА ВОНИ МОЖУТЬ БУТИ ВИКОРИСТАНІ ДЛЯ РОЗСИЛКИ ТА ІНШОГО

Зображення 9: веб-сайт “Європейської солідарності”, реєстраційна форма “Приєднуйся!” з полем для надання згоди, скріншот від 15.07.2019.

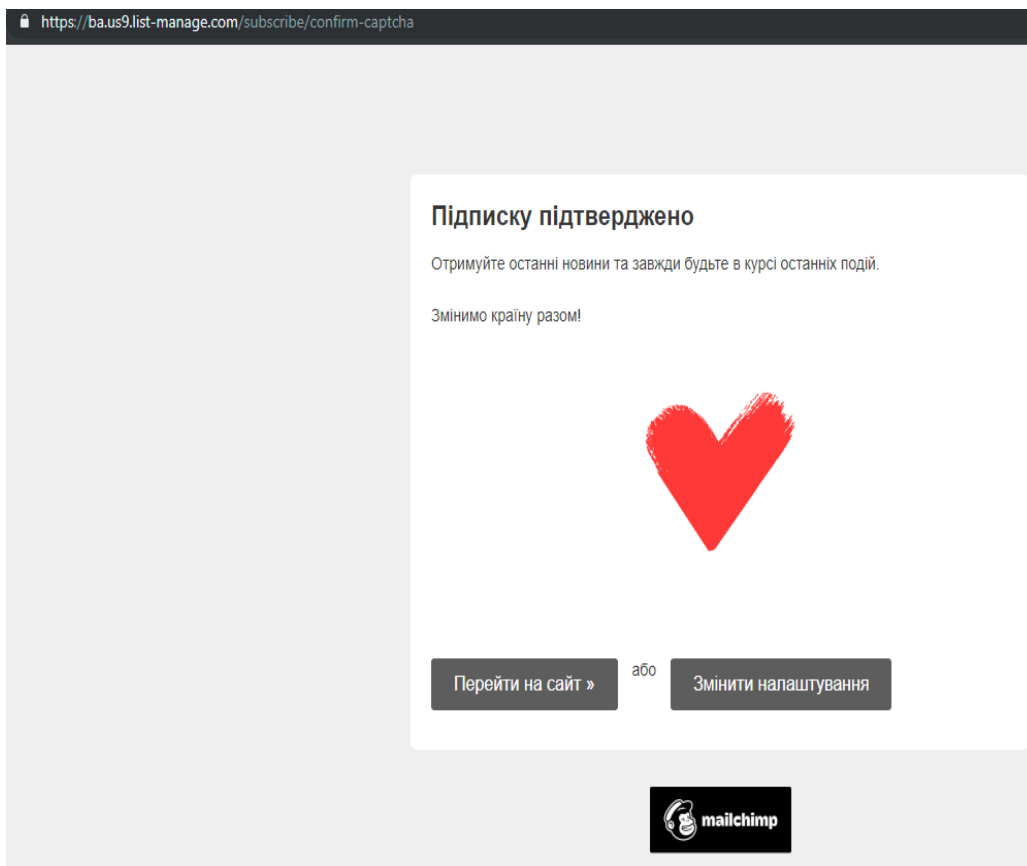
Веб-сайт “Батьківщини” пропонував відвідувачам опцію “Долучитися”, що включала членство в партії або волонтерство та можливість підписки на електронну розсилку. Волонтери могли зареєструватися онлайн. Для цього вони мали надати своє повне ім’я, телефонний номер, область, в якій вони проживають, та будь-яку іншу інформацію про себе, яку вважали потрібною (Зображення 10), заповнивши форму з обов’язковими й необов’язковими полями. Потенційні партійні члени мали надати аналогічну інформацію онлайн, а також доставити заповнену заяву в друкованому вигляді до найближчого офісу партії. Перед реєстрацією їм пропонували переглянути статут партії та її передвиборчу програму.



The image shows a screenshot of a web browser displaying the registration page for becoming a volunteer. The browser's address bar shows the URL: web.archive.org/web/20190721221109/https://ba.org.ua/stati-volonterom/. The page title is "Стати волонтером". The form contains several input fields: "Ваше ім'я (обов'язково)", "По-батькові", "Область", "Ваш email (обов'язково)", "Ваш телефон (обов'язково)", and a large text area for "Про себе". A "Надіслати" button is located at the bottom of the form. The browser's address bar also shows "94 captures" and a date range from "30 Jun 2019" to "18 Dec 2019".

Зображення 10: веб-сайт “Батьківщини”, реєстраційна сторінка “Стати волонтером”, архів від 21.07.2019, скріншот від 4.03.2020.

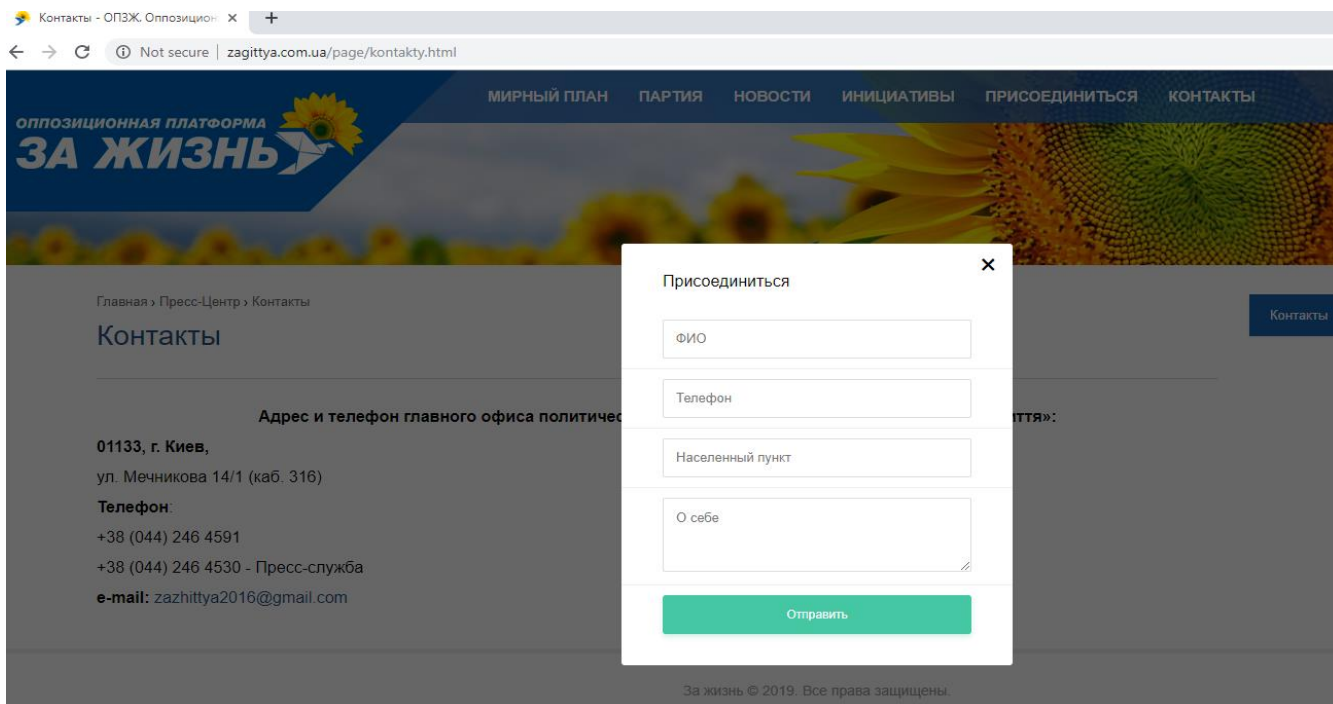
Ті, хто бажав підписатися на електронну розсилку, мали лише надати свою електронну адресу, після чого їм представляли стандартний дисклеймер MailChimp, який підтверджував, що їхню адресу було додано до електронного поштового сервісу (Зображення 11). Хоча особисте заповнення такої форми передбачає, що користувач робить це добровільно та усвідомлює мету своїх дій, партія жодним чином не інформувала їх про те, як оброблятимуться дані. Ми також не знайшли нічого, що нагадувало б політику конфіденційності на веб-сайті.



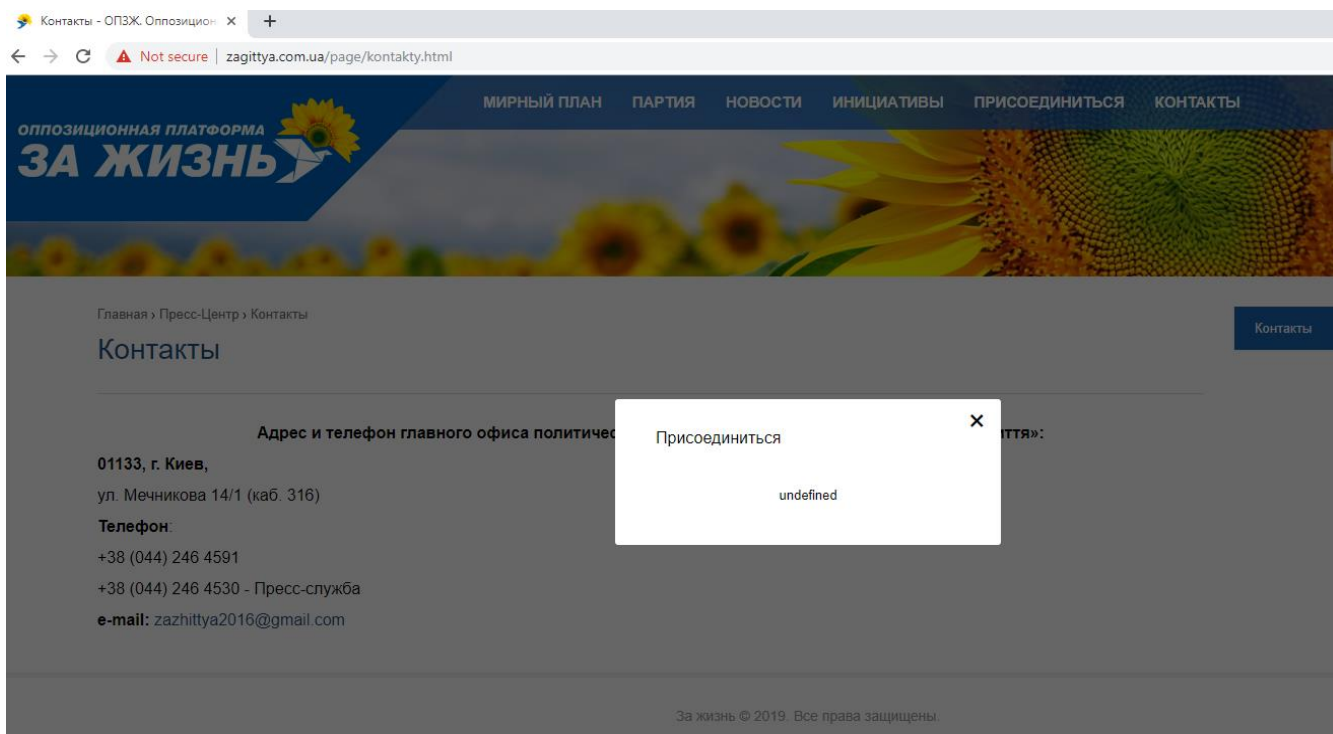
Зображення 11: веб-сайт “Батьківщини”, підтвердження Mailchimp про підписку на електронну розсилку, скріншот від 21.07.2019.

Ретроспективний огляд архівних версій веб-сайту показав, що він використовував Google Analytics, а останній аналіз – велику кількість cookies, пов’язаних з іншими соціальними медіаплатформами (такими як Youtube).

“Опозиційна платформа – За життя” вела два веб-сайти, але лише один з них був (і залишається) діючим протягом виборів, у той час як другий знаходиться “на оновленні” і пропонує відвідувачам звертатися до діючого сайту. Протягом кампанії кнопка “Приєднатися” відкривала реєстраційну форму з проханням надати своє повне ім’я, телефонний номер, місто проживання і декілька слів про себе. Партія ніде не уточнювала, в якому саме статусі “приєднується” користувач, коли заповнює форму (Зображення 12-13).



Зображення 12: “Опозиційна платформа – За життя”: розділ “Приєднатися”, спливаюче вікно для реєстрації, скріншот від 16.07.2019.



Зображення 13: “Опозиційна платформа – За життя”: розділ “Долучитися”, підтвердження реєстрації, скріншот від 16.07.2019.

Ретроспективний аналіз веб-сайту (архівна версія від 24 лютого 2019 року) виявив окрему опцію вступу до партії шляхом онлайн-реєстрації, яка запитувала більш детальну інформацію (але ми не змогли підтвердити, що ця опція була активована в період виборів). Щоб стати членом партії, користувач мав надати детальну інформацію про себе,

включаючи повне ім'я, точну адресу проживання, вид діяльності, дату народження, телефонний номер, електронну адресу, а також мав підтвердити своє прагнення стати членом партії в окремому полі. Більшість полів для заповнення були відмічені як обов'язкові (зображення 14-15). Партія також зазначала, що перед тим, як подавати заяву, користувачу варто ознайомитися зі Статутом і програмою партії.

Отже, для того, щоб стати членом політичної партії «За життя», вам необхідно заповнити форму, надавши такі дані:

1. П.І.Б. (прізвище, ім'я, по батькові)
2. Дата народження
3. Домашня адреса (обов'язково вказати індекс)
4. Телефон (за бажанням)
5. Електронна адреса (за бажанням – якщо ви хочете отримувати розсилку новин, анонси заходів та іншу інформацію із життя Партії)
6. Соціальний статус (професія)
7. «Я хочу **долучитися до лав партії «За життя»**»

Якщо ви не отримали відповідь, або з якихось інших причин отримали відмову, повідомляйте про це на електронну пошту zazhitya2016@gmail.com головного офісу політичної партії «За життя».

УВАГА! Всі поля, вказані у формі, заповнювати ОБОВ'ЯЗКОВО!

Прізвище*

Ім'я*

По батькові*

01.01.1999

Почтовий індекс*

Область*

Район*

Назва населеного пункту*

Зображення 14: “Опозиційна платформа – За життя”, сторінка реєстрації для набуття партійного членства з полями для заповнення персональних даних, архів від 26.02.2019, скріншот від 04.03.2019.

← → ↻ web.archive.org/web/20190226185407/http://zagittya.com.ua/candidates

INTERNET ARCHIVE 120 captures 19 May 2017 - 28 Aug 2019

Название населенного пункта*

Название улицы*

Номер дома*

Номер квартиры*

380

Email*

Професія*

Повідомлення

Долучитися до партії

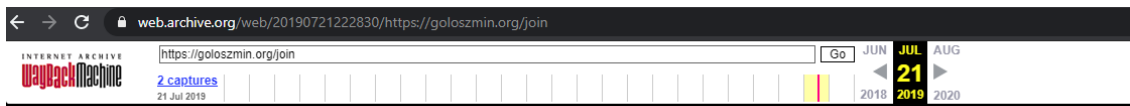
Поля із * обов'язкові для заповнення

Зображення 15: “Опозиційна платформа – За життя”, сторінка реєстрації для набуття партійного членства з полями для заповнення персональних даних (продовження), архів від 26.02.2019, скріншот від 04.03.2019.

Ретроспективний аналіз також продемонстрував, що веб-сайт використовував Google Analytics і трекер з українського розважального порталу та сервісу електронної розсилки Bigmir.net. Ніде на сайті ми не знайшли політики конфіденційності або поля для надання згоди на обробку персональних даних відвідувачів.

Партія “Голос” запропонувала найдетальнішу [політику конфіденційності](#) з двох партій, які її сформулювали (серед п’яти парламентських партій, про які йде мова в цьому дослідженні). Хоча наразі на їхньому веб-сайті вона недоступна, ми аналізували [архівну версію](#) на день виборів – 21 липня 2019 року. Наприклад, в документі йшлося про те, яка інформація збирається, а яка – ні, з якою метою та період зберігання конкретних даних. Водночас, документ надавав перелік аналітичних сервісів (третіх сторін) та cookies, що використовуються (враховуючи Facebook, Twitter та інші соціальні медіаплатформи, сервіс Google Analytics тощо) та навіть інструкцію про те, як їх вимкнути. Окрім цього, партія акцентувала на правах користувачів, що стосуються їхніх персональних даних, наприклад, право доступу до своєї персональної інформації, яку збрала партія. Ретроспективно ми не змогли підтвердити, які саме треки використовувалися протягом виборчого періоду. Зараз веб-сайт застосовує аналітичні сервіси Google Analytics та Hotjar, також cookies, якими керується Facebook та які відстежують поведінку користувача в мережі з рекламною метою. Втім, користувач про це дізнався б, лише якби прочитав політику, а не в момент відвідування сайту.

Протягом періоду передвиборчої кампанії партія набирала членів, кандидатів, волонтерів онлайн (Зображення 16), включаючи спостерігачів за виборами (Зображення 17).



ПРОГРАМА НОВИНИ КОНТАКТИ #КОМАНДАЗМІН #DIGITALKIT

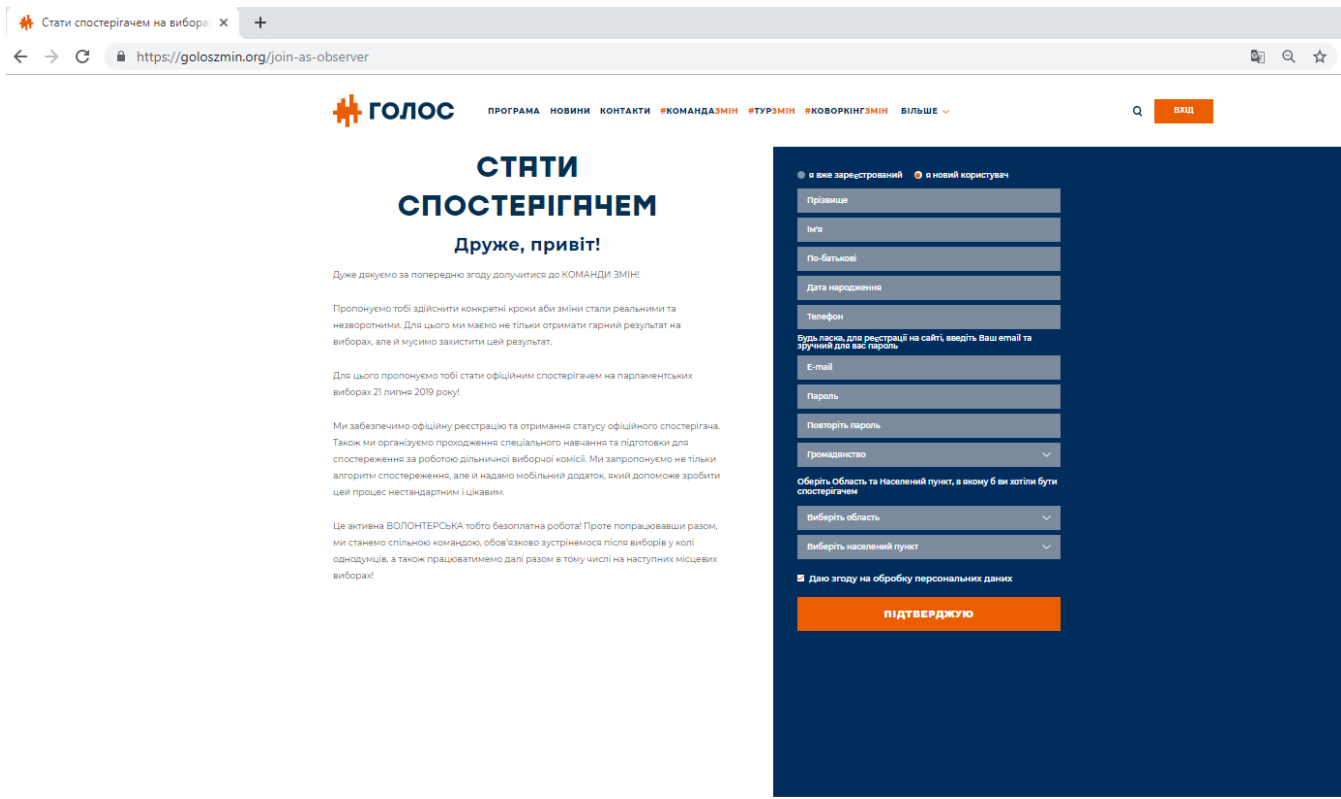
Оберіть з наведеного:

ВСТУП В ПАРТІЮ

КАНДИДАТ В НАРОДНІ ДЕПУТАТИ ПО
МАЖОРИТАРНОМУ ОКРУГУ

КАНДИДАТ В НАРОДНІ ДЕПУТАТИ ЗА
СПИСКОМ ПАРТІЇ

Зображення 16: веб-сайт “Голосу”, розділ “Приєднатись” із переліком варіантів залучення до діяльності партії: стати членом партії, стати мажоритарним кандидатом від партії або кандидатом партії зі списку, архів від 21.07.2019, скріншот від 04.03.2020.



Зображення 17: веб-сайт “Голосу”, реєстраційна форма, щоб стати спостерігачем на виборах, скріншот від 16.07.2019.

Усіх відвідувачів спочатку просили заповнити загальну реєстраційну форму і надати дані про регіон та місто їхнього проживання, ім'я, телефонний номер та електронну адресу. Після реєстрації вони отримували доступ до внутрішньої версії сайту за допомогою логіна та пароля. Така сама реєстраційна форма була ще доступна на веб-сайті станом на березень 2020 р. (Зображення 18).

Зображення 18: веб-сайт "Голосу", загальна реєстраційна форма для "приєднання" до партії з полями для заповнення даних про область та місто проживання, ім'я, телефонний номер та електронну адресу, скріншот від 04.03.2020.

4.2.1. Безпека веб-сайтів

Поверхневий аналіз веб-сайтів виявив декілька потенційних проблемних питань, з урахуванням того, що всі п'ять партій використовували свої веб-сайти для збору персональних та персональних даних своїх прихильників. Повний аналіз потребує внутрішнього доступу до партійних веб-сайтів, тому ми можемо лише розмірковувати про ризики, спровоковані цими проблемними питаннями під час виборів.

Партія	"Слуга народу"	"Європейська солідарність"	"Батьківщина"	"Опозиційна платформа – За життя"	"Голос"
URL	https://sluga-narodu.com/	https://eurosolidarity.org/	https://ba.org.ua/	http://zagittya.com.ua/	https://goloszmin.org/
Потенційні безпекові питання	Жодних не виявлено	<ul style="list-style-type: none"> • Веб-сторінка фотогалереї без шифрування завантажувала фото та робила запити до третьої 	<ul style="list-style-type: none"> • На архівній версії сайту (станом на липень 2019) використову- 	<ul style="list-style-type: none"> • Незахищене з'єднання. Веб-сайт не використовував https-протокол. 	<ul style="list-style-type: none"> • Використовувалася система керування контентом, вразлива до

		<p>сторони – хосту.</p> <ul style="list-style-type: none"> • На архівній версії сайту (станом на липень 2019) використовувалася застаріла версія 5.2.1 Wordpress з відомою на той час XSS вразливістю. • На архівній версії сайту (станом на липень 2019) використовувалася застаріла версія бібліотеки JQuery – JavaScript 	<p>валася застаріла версія 1.1.11 JQuery UI з відомою на той час вразливістю XSS.</p>		<p>різноманітних атак, включаючи XSS та RCE в минулому.</p> <ul style="list-style-type: none"> • Також використовувався дуже застарілий веб-сервер Apache 2.4.29 з одним із критичних CVE.
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Веб-сайт партії “Опозиційна платформа – За життя” використовував [незашифрований HTTP-протокол](#), який вважається небезпечним, адже потенційно залишає усі дані у вільному доступі для неуповноважених сторін у разі, якщо останні відслідковуватимуть з’єднання. База даних Загальних вразливостей та незахищеності (CVE) відзначає, що програмне забезпечення серверу було [дещо застарілим](#) під час нашого огляду в травні 2020, але жодних проблем під час виборів помічено не було. Втім, під час написання цього дослідження зв’язок із сайтом зашифрованим ще не був.

Архівна версія веб-сайту “Європейської солідарності” станом на [21 липня 2019 року](#) зафіксувала використання застарілої версії Wordpress 5.2.1 з відомою на той час вразливістю XSS, яка могла надати третім сторонам змогу вводити в оману користувачів і отримувати їхні персональні дані. Втім, ця вразливість могла бути пом’якшена адміністраторами сайту. Те саме стосується застарілої версії 1.12.14 JQuery – бібліотеки JavaScript.

Архівна версія веб-сайту “Батьківщини” станом на [21 липня 2019 року](#) продемонструвала застосування застарілої версії 1.1.11 JQuery UI з відомою на той час [вразливістю XSS](#). Інші відомі вразливі місця можуть призводити до відмови сервісу, але не до втрати чи перехоплення даних користувачів.

Система керування контентом, яку використовував веб-сайт “Голосу”, була вразлива до різноманітних атак, включаючи XSS та RCE в минулому, але конкретні слабкості системи нам невідомі. Наш огляд в травні 2020 показав, що партія використовувала сильно застарілий вебсервер Apache 2.4.29 з однією з критичних [CVE](#). Водночас, доменна історія імен продемонструвала, що з 1 травня 2019 до 15 листопада 2019 партія розміщувала свій веб-сайт на спільній хостинговій платформі, забезпеченій OVH, що зробило його ще вразливішим до слабкостей, про які ми згадували вище.

Закон про захист персональних даних зумовлює посилення захисту персональних даних про політичні погляди та зв'язки особи (стаття 7). Окрім цього, стаття 24 зобов'язує суб'єктів, які обробляють персональні дані, захищати їх від випадкової втрати або руйнування, а також від незаконної обробки, включаючи протиправне знищення або доступ до них. Отже, політичні партії мають забезпечити реальну спроможність власних веб-сайтів захищати дані користувачів від перехоплення чи втрати.

Логічно, що такий захист вимагатиме використання безпекових протоколів, оновленого програмного забезпечення тощо. Але закон не визначає ні точні безпекові заходи, яких має бути вжито, ні пояснює (аналогічно до Загального регламенту захисту даних - GDPR⁸), що заходи мають бути [“відповідними” до ризиків](#), які постають під час обробки таких даних. Своєю чергою, коли мова йде про безпеку веб-сайту або захист інших онлайн-інструментів, партії залишаються наодинці зі своїм розумінням питань безпеки та діють на власний розсуд. В умовах нерівних ресурсів та великої кількості інших пріоритетів, не дивно, що питання безпеки не завжди посідає перше місце. До того ж, рівень обізнаності про важливість цифрової безпеки на виборах доволі низький, і є лише декілька безкоштовних джерел інформації, в яких партії можуть ознайомитися з [основами проведення цифрових кампаній](#) або отримати [перелік необхідних кроків для забезпечення цифрового захисту](#).

Показово, що через чотири дні після виборів **“Голос”** [повідомив](#) про те, що їхній CRM-сервер постраждав від кібератаки групи хакерів-активістів, що називають себе **“Українським кібер-альянсом”** (УКА), відомим через злам системи проросійських бойовиків на Донбасі, атаку на російські пропагандистські платформи та [витік електронних листів](#) кремлівського високопосадовця Владислава Суркова. Виявилось, що атака проти **“Голосу”** була неофіційним тестом на проникнення, виконана в рамках флешмобу [#FuckResponsibleDisclosure](#), що має на меті публічно засоромити українських політиків за зневагу до належних безпекових заходів. Цей інцидент був оприлюднений, адже **“Голос”** одразу ж повідомив всі подробиці (Зображення 19) та відзначив, що проводиться розслідування щодо того, чи мав місце фактичний витік персональних даних користувачів, а УКА підтвердив, що виявлені слабкі місця були швидко виправлені партією (Зображення 20).

⁸ General Data Protection Regulation (GDPR) – «Загальний регламент захисту даних» – постанова Європейського Союзу про посилення та уніфікацію методів захисту персональних даних усіх осіб, що знаходяться в ЄС.

Цей інцидент наочно демонструє, наскільки серйозними могли бути наслідки кіберзламу, з урахуванням природи зібраних персональних даних та обсягу передвиборчої кампанії. Ті, хто мінімізує ресурси, направлені на безпеку, залишаються особливо вразливими до атак.

4.3. Інші методи збору даних в рамках цифрової агітації: Facebook, Google-форми, електронні розсилки, петиції тощо

Усі п'ять партій проводили активну агітацію в соціальних медіа, особливо у Facebook, де кожна партія вела офіційну сторінку, інколи пов'язану із великою кількістю напівофіційних або неофіційних сторінок і груп (включаючи регіональні сторінки або індивідуальні сторінки кандидатів). Партії використовували соціальні медіа для активної взаємодії з виборцями, особливо коли просили їх надати певну інформацію про себе, яка потім могла бути використана в таргетованій рекламі або для електронних розсилок.

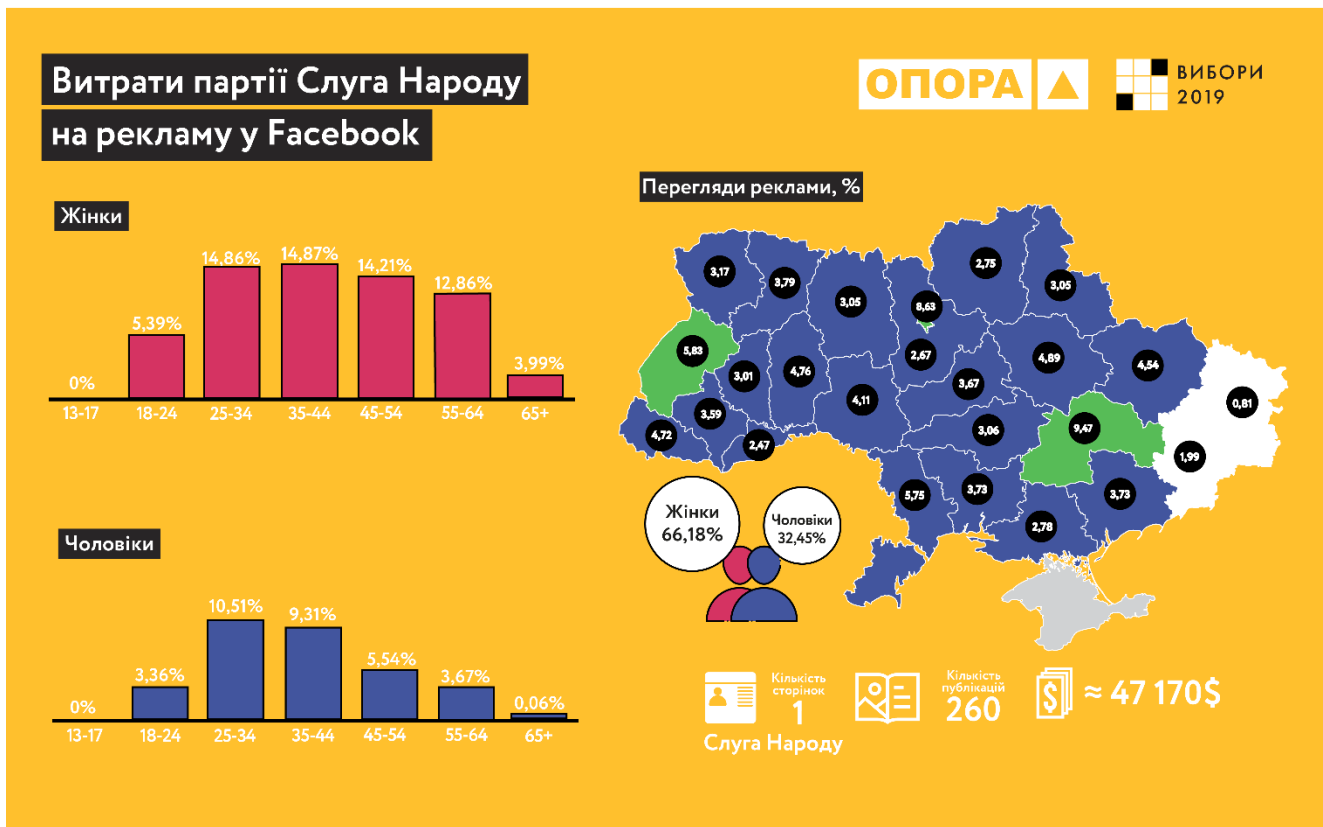
Такі методи взаємодії включали заохочення користувачів підписуватися на електронну розсилку партії, реєструватися для участі в різноманітних подіях, заповнювати Google-форми, підписуватися на події у Facebook або створювати власні, підписувати електронні петиції, переходити за посиланням на реєстраційні форми на веб-сайті для майбутніх членів чи волонтерів партії. Щонайменш дві партії (“Батьківщина” та “Слуга народу”) активували кнопку “Sign Up” на своїх Facebook-сторінках.

Згідно з даними бібліотеки політичної реклами Facebook та аналізу, [проведеному “ОПОРОЮ”](#)⁹, “Голос” опублікував найбільшу кількість постів, в яких закликав своїх прихильників реєструватися на події через Facebook, Google-форми та веб-сайт.

У той час як декілька партій публікували на свої веб-сайтах політики конфіденційності або просили користувачів дати згоду на обробку їхніх персональних даних, якісних спроб зробити те саме під час збору інформації через соціальні медіа або інші інструменти збору даних (такі, як Google-форми, онлайн-петиції або інструменти електронної розсилки) було значно менше.

Згідно з даними з бібліотеки політичної реклами Facebook, проаналізованою “ОПОРОЮ”, **партія “Слуга народу” витратила близько [47 тис. доларів США](#)** на таргетовану політичну рекламу з широким географічним охопленням, спрямовану більше на жінок, ніж на чоловіків (Зображення 21).

⁹ Згідно аналізу даних Facebook “ОПОРОЮ”.



Зображення 21: політична реклама “Слуги народу” на Facebook протягом парламентських виборів 2019 року, інфографіка ОПОРИ.

Водночас, з-поміж усіх рекламних оголошень ми знайшли лише три на офіційній сторінці Facebook, в яких партія закликала прихильників реєструватися та розповісти про проблемні питання в їхній місцевості відповідному кандидату через мобільний додаток або через веб-сайт, які коштували партії від 300 до 1 500 доларів США (більше оголошень про мобільний додаток давалися на партійних регіональних сторінках або облікових записах кандидатів).

Мажоритарні кандидати, які також користувалися рекламою на Facebook, часто закликали своїх виборців реєструватися як відвідувачів подій, волонтерів або спостерігачів за виборами через самостворені Google-форми. У таких випадках деякі кандидати додавали [детальний дисклеймер](#), в якому посилалися на норми українського законодавства, що стосуються захисту персональних даних (Зображення 22-24), інші ж – просто [просили користувачів поставити позначку згоди](#) у відповідному полі (Зображення 25), а решта взагалі [не робили нічого](#) подібного (Зображення 26).

Зе! депутат
слуга народу
 Ганна Бондар округ 220

Вітаю в Зе.Команді! 220 округ

Розкажи про себе, щоб долучитися!
Спамити не будемо
220 округ: Виноградар, Поділ, Куренівка, Мостицький і Вітряні Гори

* Required

Ім'я *

Прізвище *

Твоя громада *

- Виноградар
- Поділ
- Куренівка
- Мостицький
- Вітряні Гори

Вік *

- 18-25
- 26-35
- 36-45
- 46-55
- 56-65
- 66 і більше

e-mail *

Телефон *

У форматі 05012345678

Род зайнять *

- студент
- працюю по найму
- підприємець
- пенсіонер
- держслужбовець
- військовий
- Other:

Зображення 22-23: Google-форма кандидата від партії "Слуга народу" на 220-му окрузі для реєстрації волонтерів під час парламентських виборів 2019 року: скріншот від 07.05.2020.

Other:

Оберіть як хочете допомогти! *

- повісити банер на балконі
- розповісти про нас 10 друзям
- розкидати у своєму під'їзді нашу вітацію
- роздавати листівки біля метро та зупинок (нарайони!)
- хочу розважатися в шатрі кандидата
- хочу прийти на пікнік
- хочу бути спостерігачем на дільниці в день голосування (всьому навчимо!)
- член ДВК (якщо ви вже маєте цей досвід)
- Other:

*

Я підтверджую, що відповідно до Закону України «Про захист персональних даних» добровільно надаю політичній партії «Слуга народу» свою згоду на обробку, зберігання та використання протягом необхідного терміну моїх персональних даних згідно з цією анкетою. Своєю підписом я підтверджую, що повідомлений(а) про включення моїх персональних даних до бази персональних даних, цієї обробки персональних даних та осіб, яким передаються мої персональні дані, а також про свої права, передбачені ст. 8 Закону України «Про захист персональних даних». Я не вимагаю здійснення повідомлення про передачу (поширення) моїх персональних даних, що включені до вказаної бази персональних даних, третім особам, якщо така передача (поширення) відбувається в моїх інтересах виключно з вказаною метою, а саме безоплатна участь в діяльності політичної партії «Слуга Народу»

Підтверджую

Submit

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Зображення 24: Google-форма кандидата від партії "Слуга народу" на 220-му окрузі для реєстрації волонтерів під час парламентських виборів 2019 року (продовження): скріншот від 07.05.2020.

Волонтери команди "Слуга народу"

Хочеш стати частиною команди "Слуга народу" в 68 виборчому окрузі (Ужгородський р-н), заповни форму і з тобою зв'яжеться наш менеджер.

* Required

ПІБ *

Your answer

Номер телефону *

Your answer

Згода на обробку персональних даних *

Підтверджую

Submit

Never submit passwords through Google Forms.

This form was created outside of your domain. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Зображення 25: Google-форма кандидата від партії "Слуга народу" на 68-му окрузі, яка використовувалася для реєстрації волонтерів під час парламентських виборів 2019 року: скріншот від 08.05.2020.

Слуга Народу - Ігор Фріс - округ 84

Дякуємо за небайдужість! Заповніть форму та долучайтесь до команди розвитку!
Зробимо їх разом!

* Required

Вкажіть ваше ім'я та прізвище *

Your answer

Залиште ваш номер телефону, і ми з вами сконтактуємо *

Your answer

Submit

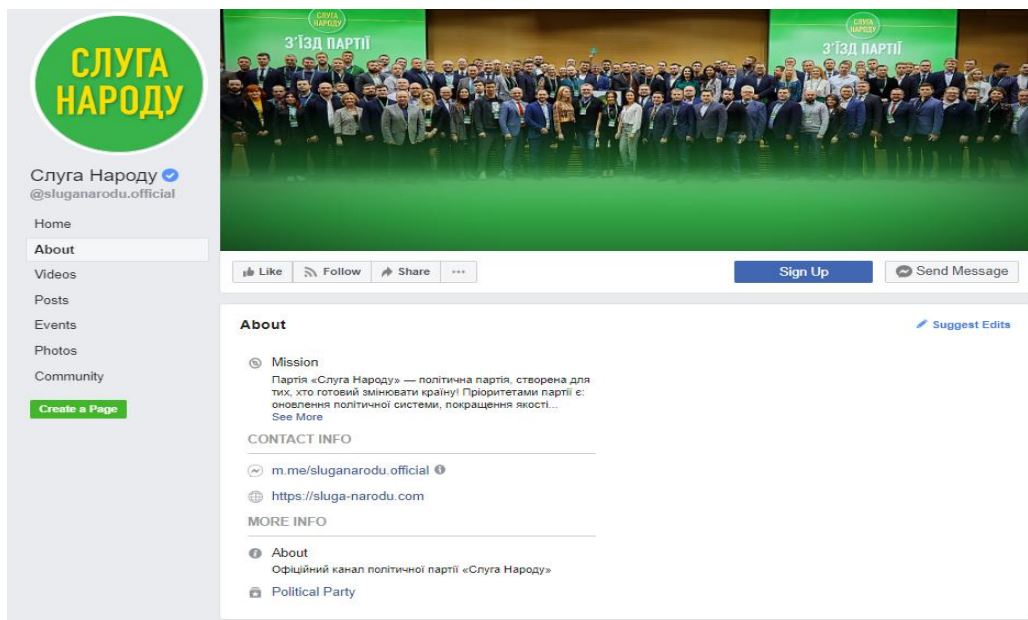
Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

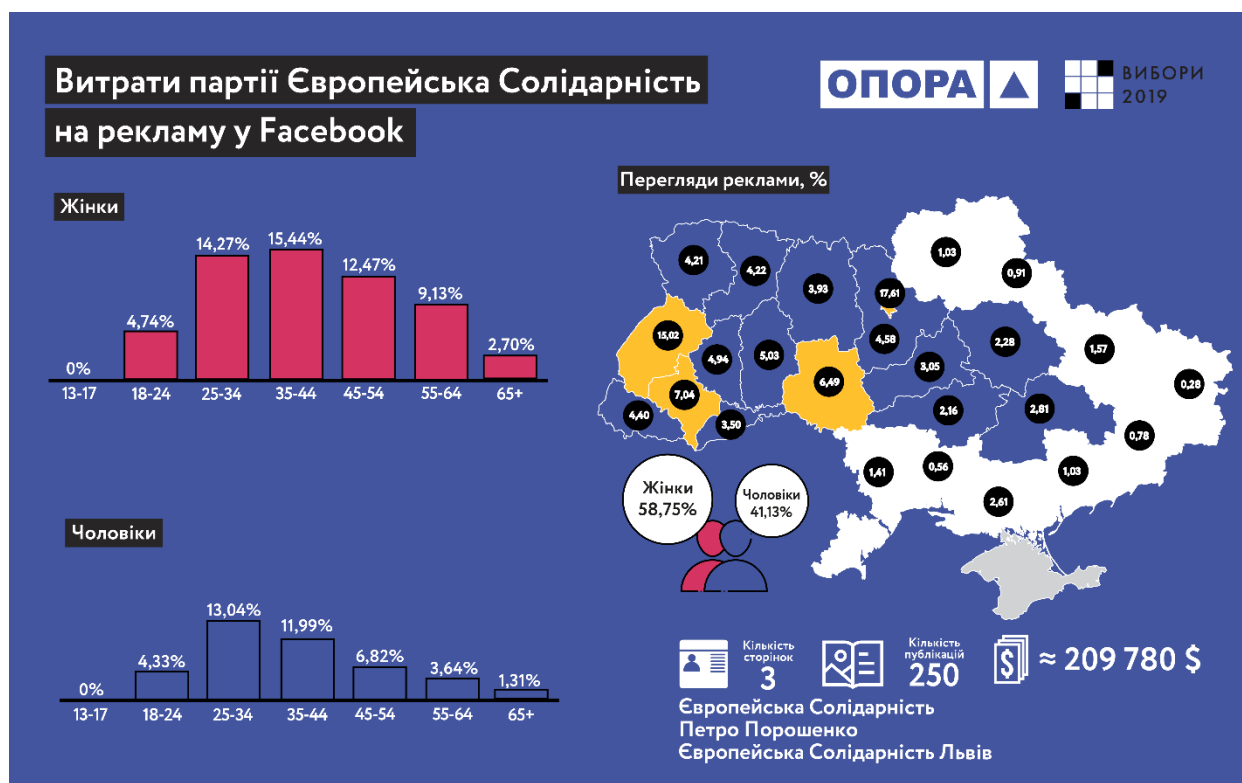
Зображення 26: Google-форми кандидата від партії "Слуга народу" на 84-му окрузі, яка використовувалася для реєстрації волонтерів під час парламентських виборів 2019 року: скріншот від 08.05.2020

Партія "Слуга народу" також використовувала кнопку "Sign Up" на своїй Facebook сторінці, щоб переправляти користувачів до розділу "Приєднатись" на веб-сайті партії, який вже було описано вище (Зображення 27).



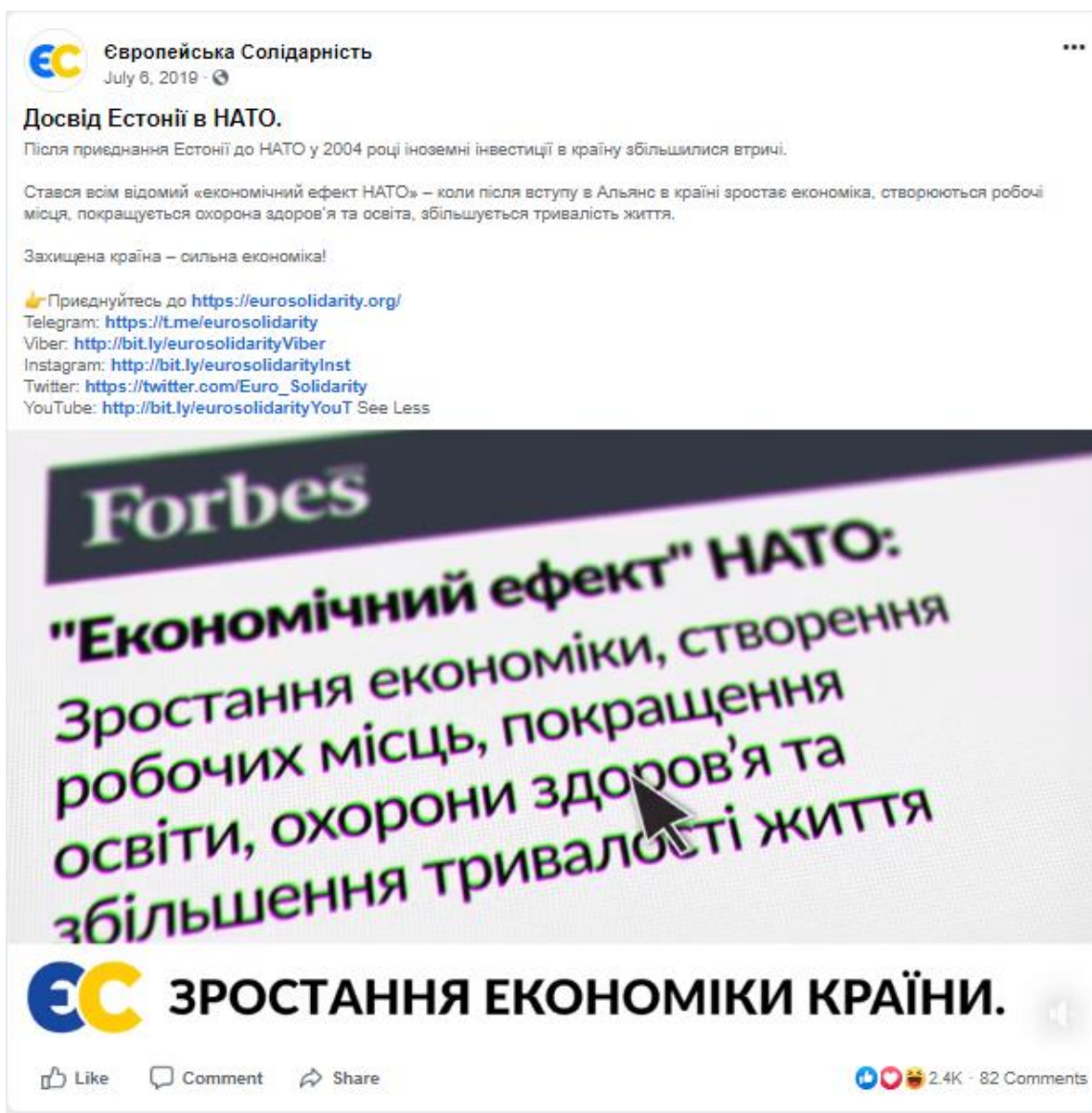
Зображення 27: кнопка “Sign Up” (“Підписатися”) на офіційній сторінці Facebook партії “Слуга народу”, скріншот 19.03.2020

“Європейська солідарність” також проводила активну кампанію на Facebook і витратила понад 200 тис. доларів США на політичні рекламні оголошення на платформі, які були трохи більше спрямовані на жінок, ніж на чоловіків, а в географічному вимірі – на західну і центральну Україну (Зображення 28).



Зображення 28: політичні рекламні оголошення на Facebook партії “Європейська солідарність” протягом парламентських виборів 2019 року, інфографіка “ОПОРИ”.

Хоча ми не змогли підтвердити, чи використовувала партія на своїй сторінці кнопку із закликом до дії в будь-який з моментів кампанії, вона закликала прихильників приєднуватися через веб-сайт та підписуватися на її облікові записи на інших соціальних платформах (Зображення 29). Проте ми не знайшли рекламних постів, які заохочували б виборців реєструватися або залишити свої персональні дані на офіційній сторінці партії й двох пов'язаних з нею сторінок, з яких публікувалися політичні оголошення від імені партії (сторінка Петра Порошенка та львівська сторінка “Європейської солідарності”).

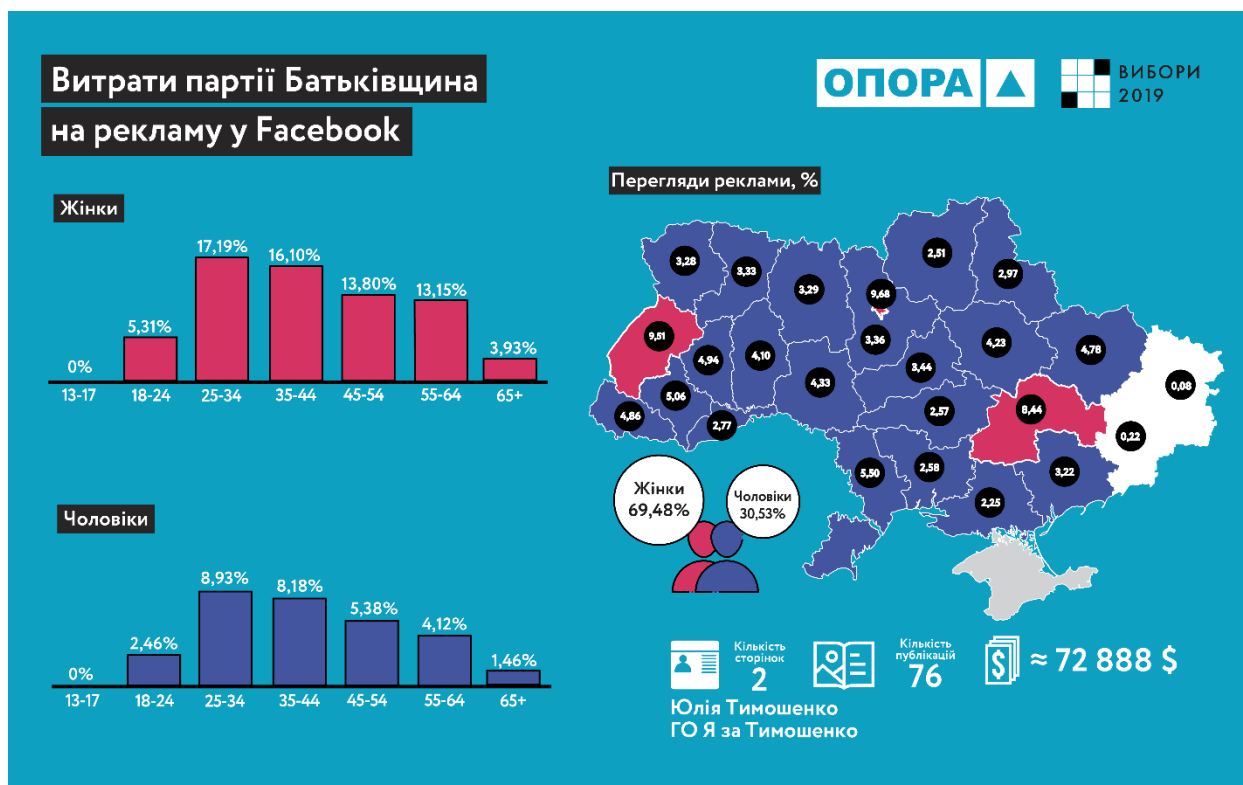


Зображення 29: 6 липня 2019 року, пост “Європейської солідарності” на Facebook, що закликає долучатися через веб-сайт та інші соціальні мережі, скріншот від 16.03.2020.

Водночас, як мінімум з одного приводу “Солідарність” таки закликала своїх прихильників підписати онлайн-петицію. Ця петиція закликала Парламентську Асамблею Ради Європи скасувати членство та право голосу Росії в ПАРЄ. На момент написання цієї доповіді петицію, створену партією, [підписали 41 561 осіб](#). Це означає, що вона отримує персональні дані, надані кожним підписником відповідно до [політики конфіденційності](#) Change.org. Хоча Change.org вважає необхідним ділитися такою інформацією з авторами

петицій, щоб продемонструвати легітимність підписів, ініціювання онлайн-петиції може також використовуватися для збору даних про прибічників ідеї заклик, а потім застосовуватися на власний розсуд (наприклад, щоб контактувати з користувачами, які надали свої електронні адреси поза платформою петицій).

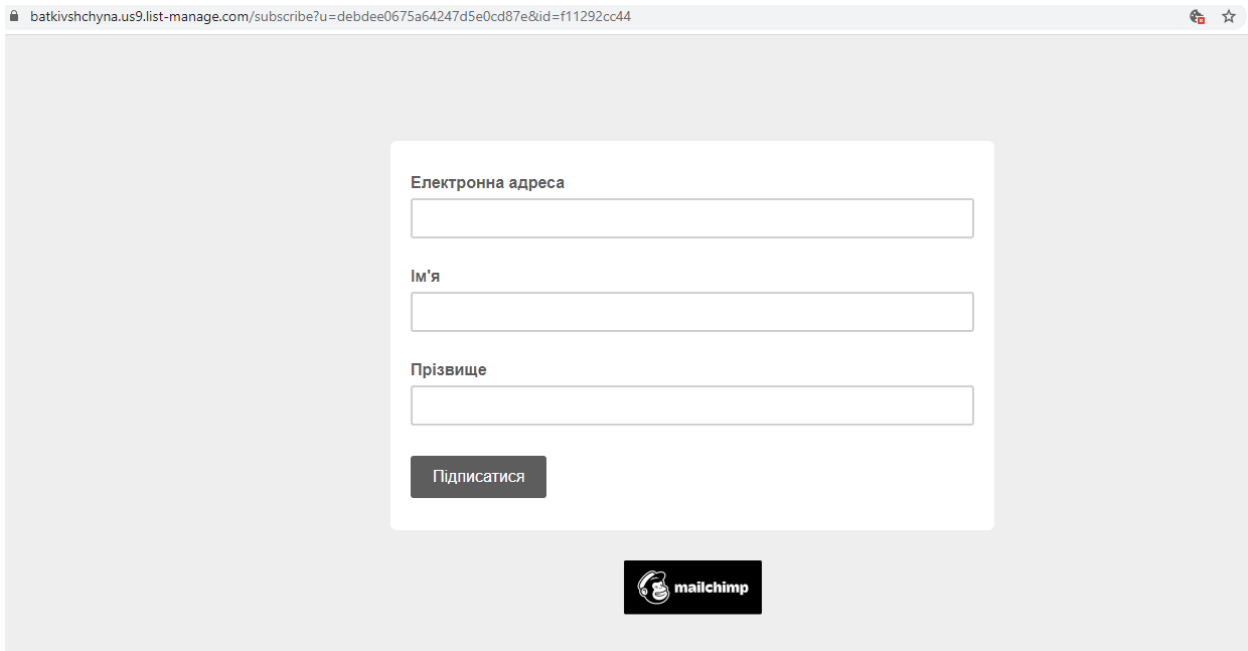
“Батьківщина” посіла четверте місце за рівнем витрат на рекламу в Facebook із сумою понад 72 тис. доларів США (Зображення 30). Оголошення були направлені більше на жінок, ніж на чоловіків та поширювалися більш-менш рівномірно в географічному вимірі. Аналізуючи партійні оголошення (які публікувалися з офіційного облікового запису лідера партії Юлії Тимошенко та партійної фан-сторінки), ми не виявили рекламних постів, які б заохочували виборців реєструватися або залишати персональні дані.



Зображення 30: політична реклама “Батьківщини” на Facebook протягом парламентських виборів 2019, інфографіка “ОПОРИ”.

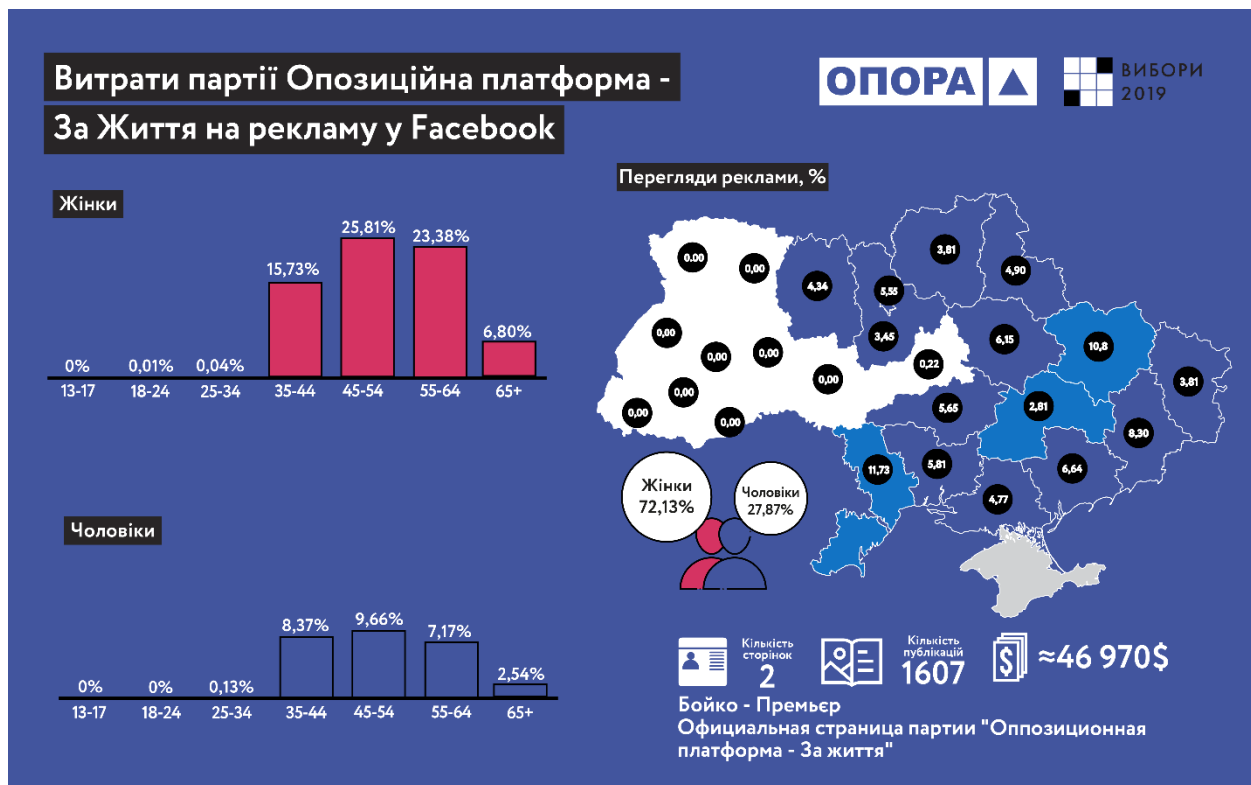
Партія використовувала на своїй основній сторінці у Facebook кнопку із закликом до дії, щоб запропонувати користувачам підписатися на електронну розсилку MailChimp. Така сама функція була ввімкнена на партійному веб-сайті. Пояснення того, як саме оброблятимуться персональні дані, теж було відсутнє.

Показово, що [політики конфіденційності](#) сервісу MailChimp відповідають Загальному регламенту захисту даних ЄС та включають специфічні поля для надання згоди на обробку персональних даних, наприклад, опція надання згоди від користувача на застосування програмного забезпечення установою та пояснення того, як вона використовуватиме дані. Натомість, під час використання сервісу “Батьківщиною”, ці функції або були недоступні для України, або ж не були ввімкнені партією (Зображення 31).



Зображення 31: форма реєстрації MailChimp, пов'язана із кнопкою із закликом до дії, на Facebook-сторінці партії "Батьківщина", скріншот від 17.03.2020.

При тому, що "Опозиційна платформа – За життя" була найменш активною в соціальних медіа, вона витратила понад 40 тис. доларів США на політичну рекламу, спрямовану на користувачів Facebook віком понад 35 років (Зображення 32).

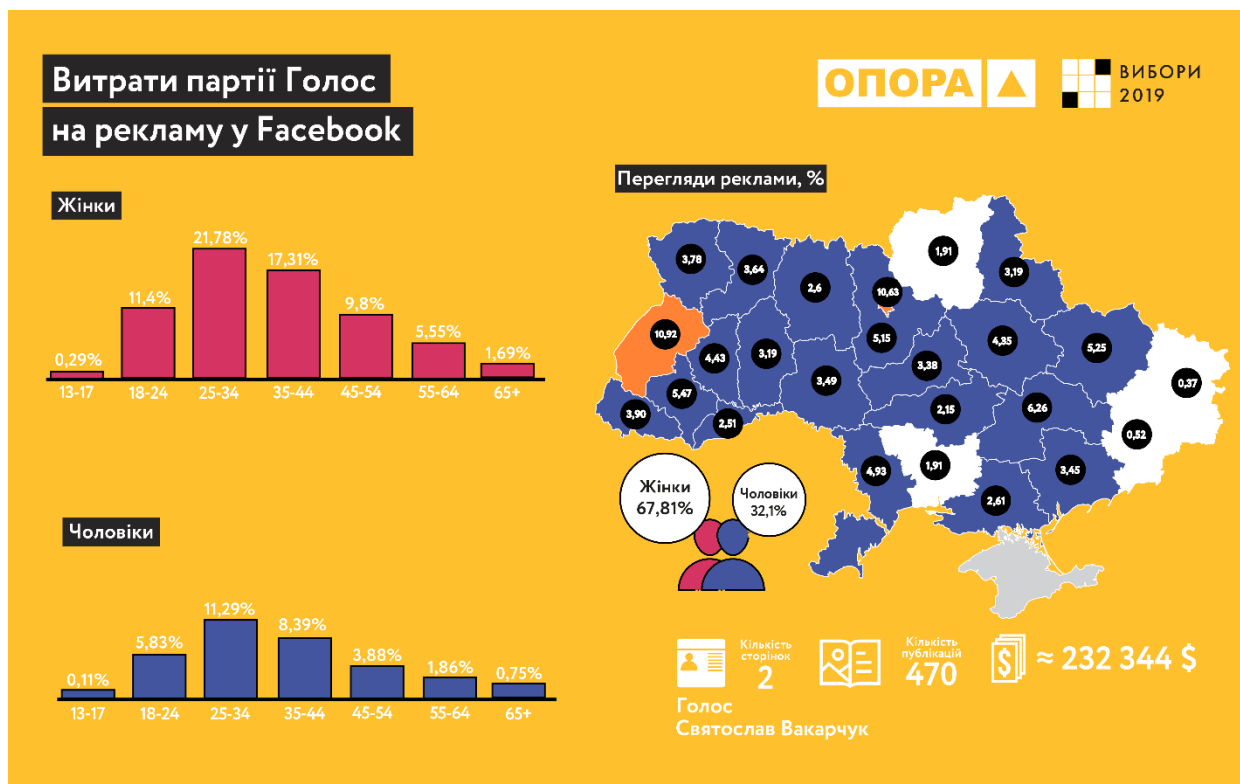


Зображення 32: політична реклама "Опозиційної платформи – За життя" протягом парламентських виборів 2019, інфографіка "ОПОРИ"

Водночас, ми не змогли виявити рекламних постів, які б містили посилання на розділ

“Приєднатися” або закликали відвідувачів зареєструватися якимось іншим чином як на офіційній партійній сторінці, так і на пов’язаній фан-сторінці (“Бойко – Прем’єр”).

“Голос” витратив на рекламу в Facebook понад 230 тис. доларів США (Зображення 33). Вона була спрямована на наймолодшу аудиторію серед всіх партій. Щонайменше 262 рекламних пости на офіційній партійній сторінці у Facebook закликали прихильників зареєструватися (надати персональні дані). Ці публікації коштували партії мінімум 41,6 тис. доларів США.



Зображення 33: Політична реклама “Голосу” на Facebook під час парламентських виборів, інфографіка “ОПОРИ”

Так, партія часто публікувала посилання на реєстраційні форми на веб-сайті, які були описані вище, та активно закликала своїх прихильників проводити [онлайн-агітацію від її імені](#). Вона також заохочувала виборців приєднуватися до партійних офлайн-подій та агітаційної діяльності, вербуючи учасників через запрошення у Facebook та Google-форми. Заявки [на статус волонтера](#) на базі Google-форм, відкриття партійного брендованого робочого простору, заявки на те, [щоб “очолити” такий простір](#), [організація тематичної](#) вечірки – всі ці реєстраційні форми, що ми виявили під час нашого дослідження, не містили посилань на політику конфіденційності “Голосу” або отримання згоди від учасників на обробку персональних даних (Зображення 34-35).

Голос в Карпатах

Прізвище та ім'я
Your answer

Місце проживання
Your answer

Дата народження
Date
mm/dd/yyyy

номер телефону
Your answer

Зображення 34: реєстраційна форма на набуття статусу волонтера “Голосу” на базі Google-форм, скріншот від 22.03.2020.

e-mail
Your answer

Я готовий

їхати волонтером та аргітувати

бути водієм на власному авто

Other: _____

У мої машині стільки місць
Your answer

Submit

Never submit passwords through Google Forms.

This form was created outside of your domain. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Зображення 35: реєстраційна форма на набуття статусу волонтера “Голосу” на базі Google-форм (продовження), скріншот від 22.03.2020.

4.4. Месенджери і чат-боти

Як було зазначено раніше, під час виборчого циклу 2019 року месенджери (такі, як Telegram), стали пріоритетом для партій та кандидатів у контексті ведення кампаній. Чотири з п'яти партій, розглянутих в цій доповіді, використовували Telegram-канали або групи для залучення виборців онлайн. До того ж, мінімум одна з цих партій використовувала Viber. Ще одна нова характеристика онлайн-залучення в 2019 році включала використання чат-ботів.

Поки Telegram-канали застосовували односторонню комунікацію (коли виборці здебільшого просто отримували інформацію про діяльність партії або кандидата), API месенджерів дозволяв третім сторонам створювати чат-боти – автоматичні Telegram-додатки для того, щоб користувач міг з ними взаємодіяти. Встановлюючи такі додатки, користувачі неминуче передавали якісь свої дані розробникам. Наприклад, у ході користування ботом, розробникам надсилалася така інформація, як публічні дані з акаунта користувача або зміст повідомлень. У своїй політиці конфіденційності Telegram зауважує, що інші боти, крім його власних (такі, що належать третім сторонам), повністю незалежні від сервісу і [мають отримати дозвіл](#) користувача, перш ніж їм буде надано доступ до персональних даних.

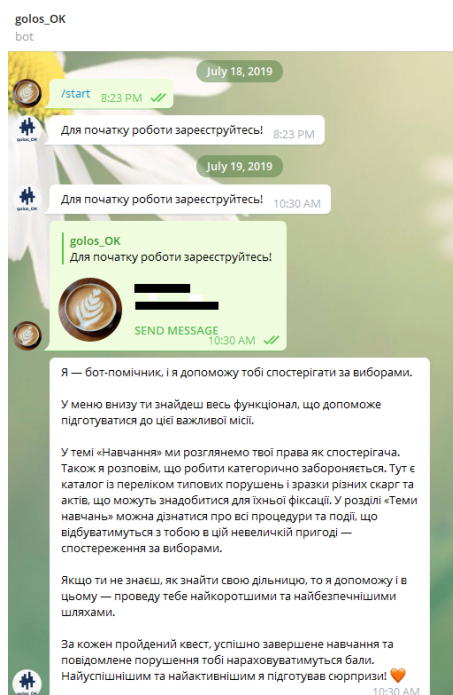
“Слуга народу” і “Голос” активно використовували чат-ботів Telegram протягом кампанії 2019 року. Наприклад, “Слуга народу” використовував його, щоб швидко відповідати на популярні запитання про партію, її кандидатів, поширювати інформацію про виборчі порушення або ймовірні “фейки”. Ми взаємодіяли з двома такими ботами, що належали різним партіям.

Так, один з ботів “Слуги народу” просив користувача надати інформацію про свій виборчий округ, щоб, у свою чергу, повідомляти йому/їй інформацію про відповідного кандидата. Бот не пропонував розглянути інформацію про збір даних або спершу надати на це згоду (Зображення 36).

“Голос” також користувався чат-ботами протягом кампанії: зокрема, ця партія створила [відкритого Telegram-бота](#) для поширення інформації про порушення виборчого процесу від акредитованих спостерігачів, а також від простих громадян. Під час взаємодії партійний бот багаторазово пропонував користувачеві “зареєструватися”. Втім, подальша комунікація проводилася без жодної інформації про збір даних або запиту про згоду користувача на використання персональних даних (Зображення 37).



Зображення 36: Telegram-бот партії “Слуга народу” для відповіді на найпопулярніші запитання, скріншот від 16.07.2020.



Зображення 37: Telegram-бот “Голосу” для моніторингу виборів, скріншот від 19.07.2020.

5. Інші джерела персональних даних громадян

В Україні існує велика кількість офіційних та неофіційних баз даних і реєстрів персональних даних громадян. Вони включають державні реєстри, скомпільовані та адміністровані державою з метою надання державних послуг, бази даних споживачів і комплексні набори даних комерційної природи, походження яких не завжди очевидне. Багато випадків, коли державні та приватні бази даних виставлялися на продаж в мережі, демонструють, що захист особистих даних громадян державними і приватними інститутами й досі залишає бажати кращого.

Хоч ми і не знайшли очевидних доказів того, що політичні партії використовували такі дані

в своїй кампанії 2019 року або намагалися їх придбати, спостерігачі за виборами зафіксували [випадки незаконного збору та використання персональних даних](#) та таргетування виборців згідно даних, яких вони [не надавали тим чи іншим політичним силам для агітації](#). Проте, на даний момент видається, що партії більше сподіваються на дані про своїх членів та прихильників, які вони збрали самостійно, навіть якщо такі практики збору даних не завжди відповідають чинним правовим нормам.

5.1. Державний реєстр виборців

Ймовірно, найповнішою базою даних про виборців в Україні є **Державний реєстр виборців**. Реєстр є автоматизованою [централізованою національною базою даних](#), створеною Центральною виборчою комісією (ЦВК) у 2009 році для обліку всіх виборців на території країни і складається з таких даних, як повне ім'я виборця, дата і місце народження, зареєстроване місце проживання та інші персональні дані всіх осіб 18-річного віку та старше, які мають право голосу згідно з законодавством. База даних утримується спеціальним органом у структурі ЦВК із застосуванням належних безпекових заходів і дозволяє вносити оновлення в режимі реального часу, а також забезпечує створення виборчих списків для виборів та референдумів на всіх рівнях. Персональні дані громадян автоматично потрапляють до Реєстру, коли вони досягають виборчого віку, що складає більше ніж 30 мільйонів записів.

Закон України “Про Державний реєстр виборців” забезпечує механізми громадського контролю, серед яких – право виборця на перегляд своїх персональних даних (онлайн та офлайн) і запит на їхню зміну. Реєстр також доступний для зареєстрованих [кандидатів в президенти](#) і [політичних партій](#), представлених в Парламенті, не пізніше ніж за 60 днів до призначеного дня виборів. Остання [процедура](#), визначена ЦВК, передбачає надання вповноваженим партійним представникам або кандидатам електронної копії повної бази даних на захищеному оптичному запам'ятовувальному пристрої. Ця процедура виконується для того, щоб вони могли провести аудит створених виборчих списків, і лише з цією метою у повній відповідності до законодавства про захист інформації та персональних даних. Згідно з цією процедурою, один призначений представник від кожної парламентської партії або кандидата в президенти може потім вивчати дані в приміщеннях ЦВК в робочий час, використовуючи обладнання та спеціалізоване програмне забезпечення, надане Комісією, і без права повного або часткового копіювання даних в будь-якій формі, включаючи з використанням фото- та відеообладнання.

Звісно, такий суворий порядок робить змістовну роботу з базою даних із понад 30 мільйонами записів жодним чином неможливою. Як сказав один з кандидатів в президенти 2019 року, йому б знадобилося понад 6 000 років, щоб [особисто провести аудит даних Реєстру](#) відповідно до умов, описаних вище. При цьому ЦВК пояснює, що такий порядок має на меті запобігти продажу або витоку даних до сторонніх осіб. Спостерігачі за виборчим процесом також закликали ЦВК [надати деперсоналізовані дані з Реєстру в форматі, зручному для машинного зчитування](#), та таким чином забезпечити можливість громадського контролю, а також подолати занепокоєння про [можливі маніпуляції зі списками виборців](#) з боку влади або учасників виборчого процесу. Але суд [визнав](#) такий обмежений доступ до Реєстру законним, аргументувавши своє рішення безпековими питаннями.

Безпеку веб-сайту Реєстру перевірів й Український кібер-альянс хакерів (у 2018 році), виявивши його вразливість до [XSS-атаки](#). Хоча ця вразливість здавалася некритичною, члени ЦВК самі визнали нестачу кваліфікованого ІТ/кібер безпекового персоналу серед співробітників ЦВК через велику різницю в заробітній платні таких спеціалістів між приватним та державним сектором.

5.2. Витоки інформації, злами та безпекові питання

Занепокоєння про безпеку і цілісність персональних даних громадян, які збираються та обробляються державними і приватними установами, піднімалося й в інших аспектах. В 2019 році під час інтерв'ю Михайло Федоров, який пізніше Міністром цифрової трансформації України, [натякав](#), що той факт, що певні державні реєстри контролюються кримінальними силами, є “перепорою” на шляху до амбітного урядового плану оцифрування державних послуг.

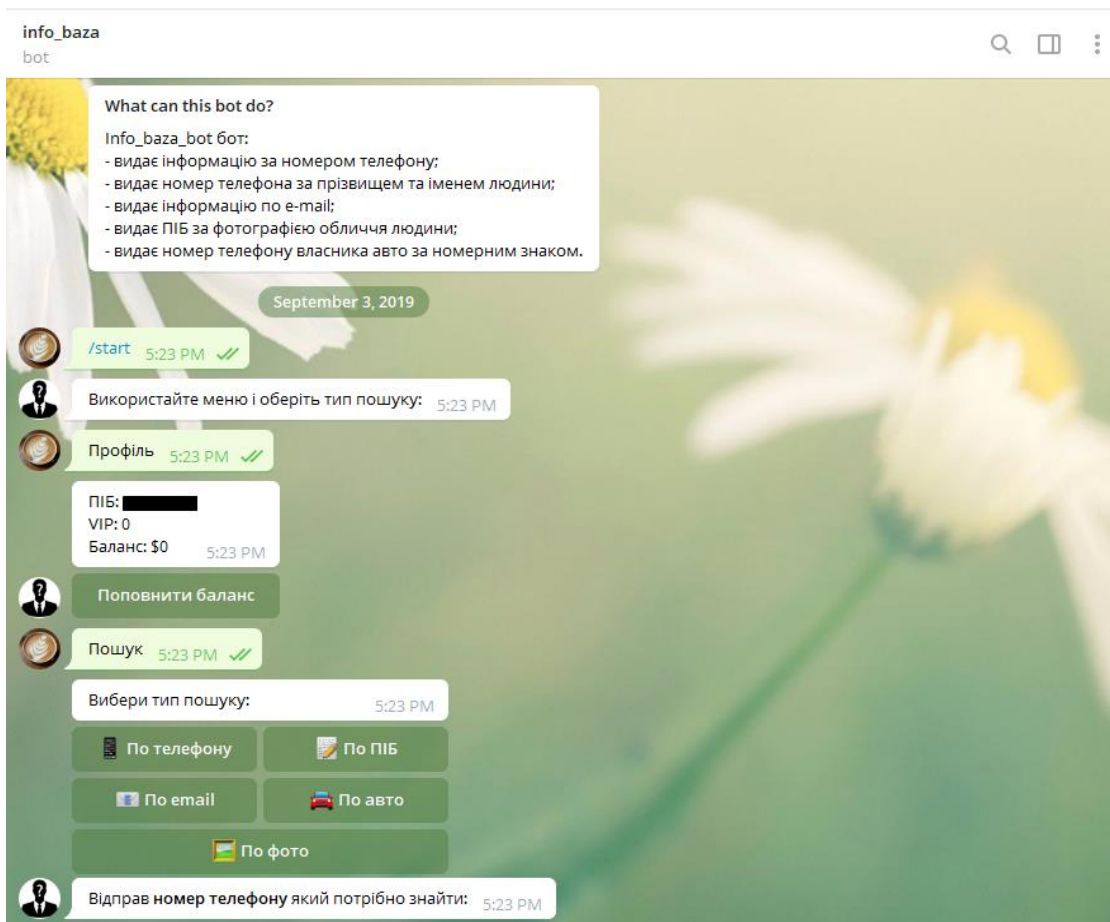
Керівництво правоохоронних установ також розслідувало справи щодо конфіденційних державних даних, що продавалися на “чорних” веб-сайтах, (наприклад, база даних [Державної митної служби України](#)). А журналісти виявили онлайн-бюлетень з десятками наборів даних, які містили інформацію про споживачів та були доступними до придбання – наприклад, база даних [18 мільйонів клієнтів](#) найбільшої української логістичної компанії або база даних клієнтів одного з найбільших банків України. Вони також натрапили на торговців даними, які [пропонували бази даних споживачів «на замовлення»](#), включаючи імена, телефонні номери, стать та електронну адресу особи. Хоча ми не маємо змоги підтвердити автентичність деяких баз даних, які досі доступні онлайн, назви файлів припускають, що вони були отримані з державних органів або провідних комерційних установ країни. В одному з нещодавніх журналістських розслідувань цього питання виявлено, що [інформація з Єдиного демографічного реєстру та Державного реєстру виборців 2014 року](#) знаходяться в продажу на нелегальному ринку.

У той час як ці факти не викликають значного занепокоєння у громадськості (окрім отримання масової смс-реклами), багато державних баз даних містять чутливу персональну і комерційну інформацію. Нещодавній інцидент в [Нових Санжарах](#) продемонстрував, як неправомірний доступ до тисяч телефонних номерів мешканців конкретного населеного пункту може використовуватися для поширення дезінформації, провокувати масову паніку і протести через популярний месенджер Viber та інші соціальні мережі.

5.3. Напівлегальні і нелегальні джерела

Важливо звернути увагу на те, що українське законодавство не містить категоричної заборони **об'єднання персональних даних громадян з різних відкритих джерел**, враховуючи, наприклад, урядові реєстри, доступні завдяки [положенням про відкриті дані](#), баз даних для пошуку роботи і дані з соціальних мереж. З'явилися компанії, які пропонують всі начебто публічно доступні дані про фізичних осіб та установи, або надають “послугу” об'єднання різних елементів цих даних.

Так, Telegram-бот, розроблений у 2019 році, прив'язує номер телефону особи до її імені або навпаки, а також шукає іншу персональну інформацію, як-то електронна пошта, фото обличчя людини або номер автомобіля (Зображення 38). Бот робить це безкоштовно або в обмін на інший телефонний номер (чи декілька) з контактів мобільного телефона користувача (вочевидь, не питаючи згоди власника). Більший обсяг даних коштуватиме скромну суму в 50 доларів США. Ті, хто створили бот (їхні особи невідомі), наполягають на тому, що їхні початкові дані були зібрані з відкритих ресурсів для пошуку роботи, але є причини вважати, що [деяка інформація з'явилася там через витоки баз даних споживачів](#). Вірогідним видається також такий сценарій, коли замість того, щоб злити всю базу даних, співробітники [державних установ](#) або [приватних підприємств](#) продають дані, до яких вони мають доступ, частинами – наприклад, як у випадках, що вже були виявлені правоохоронними органами.

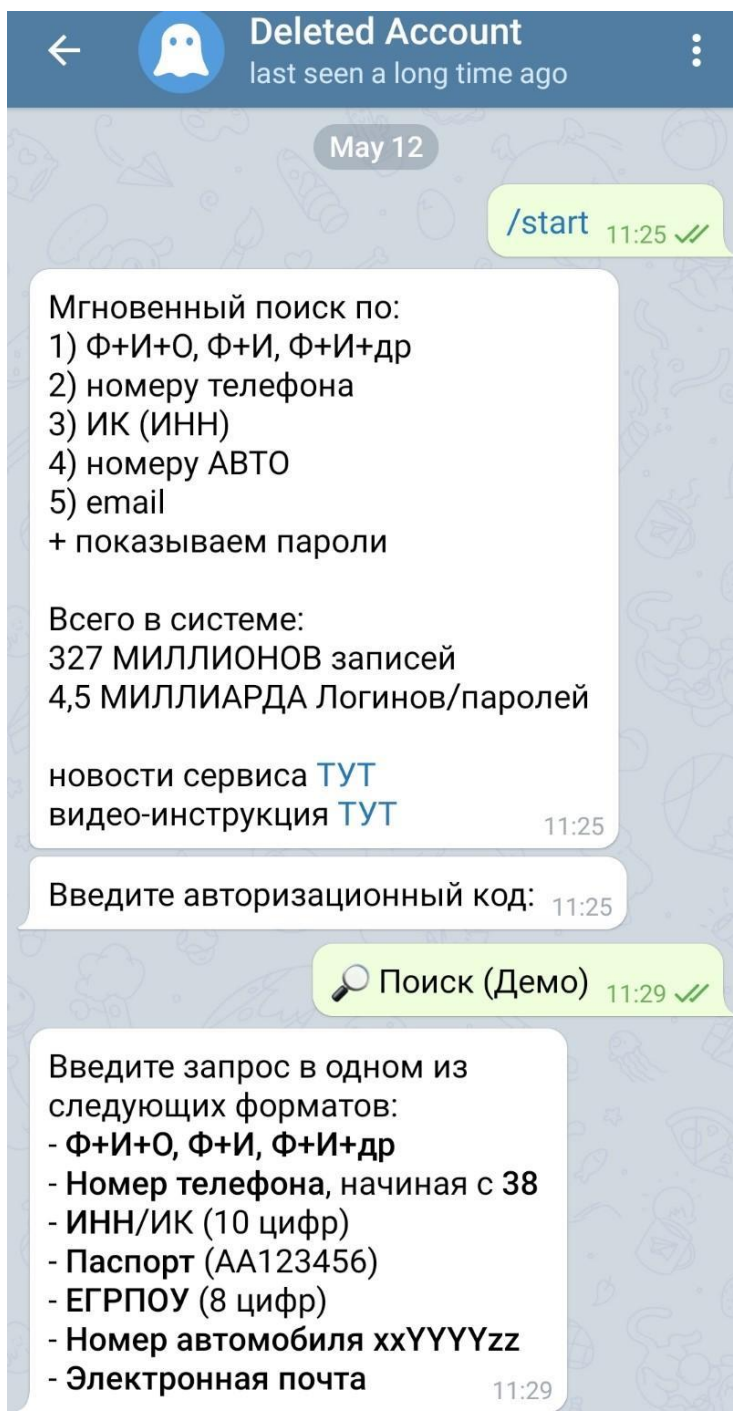


Зображення 38: можливі варіанти запиту даних бота @Info_baza Telegram, скріншот від 03.09.2019.

Під час написання цього дослідження з'явився інший анонімно створений бот @UA_Baza, який пропонує навіть більш деталізовану інформацію про мільйони громадян на продаж, включаючи такі важливі дані, як [номери паспортів, ідентифікаційні коди, зареєстровані місця проживання, паролі до соціальних мереж й навіть деталі банківських рахунків](#). Цей перелік означає, що така база даних не могла збиратися з відкритих і легально доступних онлайн-ресурсів (Зображення 39). Ще й надто, бот надає чіткі інструкції про те, як придбати дані за біткойни в еквіваленті 50 доларів США (за 10 записів).

Після громадського обурення та [офіційного розслідування](#) про те, як персональні дані

громадян опинилися в Інтернеті, оригінального бота було видалено, але пізніше його знову відтворили в мережі під багатьма іншими іменами. Розслідування прийшло до висновків, що дані були вилучені з різноманітних баз даних. Журналістське розслідування [висунуло версію](#), що дані походили з державних реєстрів, комерційних баз даних та соціальних медіа. Беручи до уваги природу таких витоків інформації, неможливо передбачити, яка саме база даних спливе на поверхню в майбутньому та яким чином вона використовуватиметься.



Зображення 39: можливі інформаційні запити від Telegram-боту @UA_baza, включаючи чутливі персональні дані, такі як номер паспорту або податковий номер, скріншот від 12.05.2020 (обліковий запис було видалено того ж дня).

5.4. Дані споживачів

В Україні є декілька компаній, які володіють величезними обсягами даних споживачів, включаючи споживачів [онлайн-магазинів](#), телекомунікаційних компаній, [банків](#), [логістичних компаній](#) тощо, які загалом збирають дані споживачів для власних цілей, хоча інколи пропонують третім сторонам ці дані в маркетингових цілях. Окрім того, працює декілька національних програм лояльності – деякі з яких охоплюють понад [90 онлайн-магазинів](#) та мільйони клієнтів з усієї України. Також існують [цифрові рекламні мережі](#), що управляють власними інформаційними платформами, які збирають та аналізують трафік веб-сайтів і дані користувачів та влаштовують аукціони в реальному часі для продажу таргетованої реклами. Менші компанії також мають бази даних клієнтів. Якщо більші бази даних споживачів інколи виставляються на продаж через злами або зливи недобросовісними співробітниками, менші бізнеси часто продають дані своїх клієнтів.

Фактично, продаж даних про споживача без інформованої згоди цього споживача є порушенням закону про захист персональних даних. Але в Україні не вистачає ефективних норм та механізмів для моніторингу таких правопорушень.

5.5. Ймовірні джерела даних виборців в політичній агітації 2019 року

Ми не знайшли жодних прямих ознак того, що політичні партії використовували бази даних споживачів чи некомерційні бази для проведення агітації або робили спроби їх придбати (але це не означає, що такі факти не мали місце). Натомість, партії розраховували, в першу чергу, на власні списки членів, а також на дані, зібрані від їхніх потенційних виборців та активістів ще до проведення виборів. У той час як наша доповідь фокусується лише на онлайн-методах збору даних, є ознаки того, що учасники виборів збирали також персональні дані офлайн, адже спостерігачі повідомляли про випадки, коли партії або кандидати робили це [під хибними приводами](#) або порушували [принцип інформованої згоди](#). Публікації в медіа свідчать, що [деякі партії ділилися базами прихильників, сформованими під час президентських виборів 2019 року](#), зі своїми кандидатами до Парламенту.

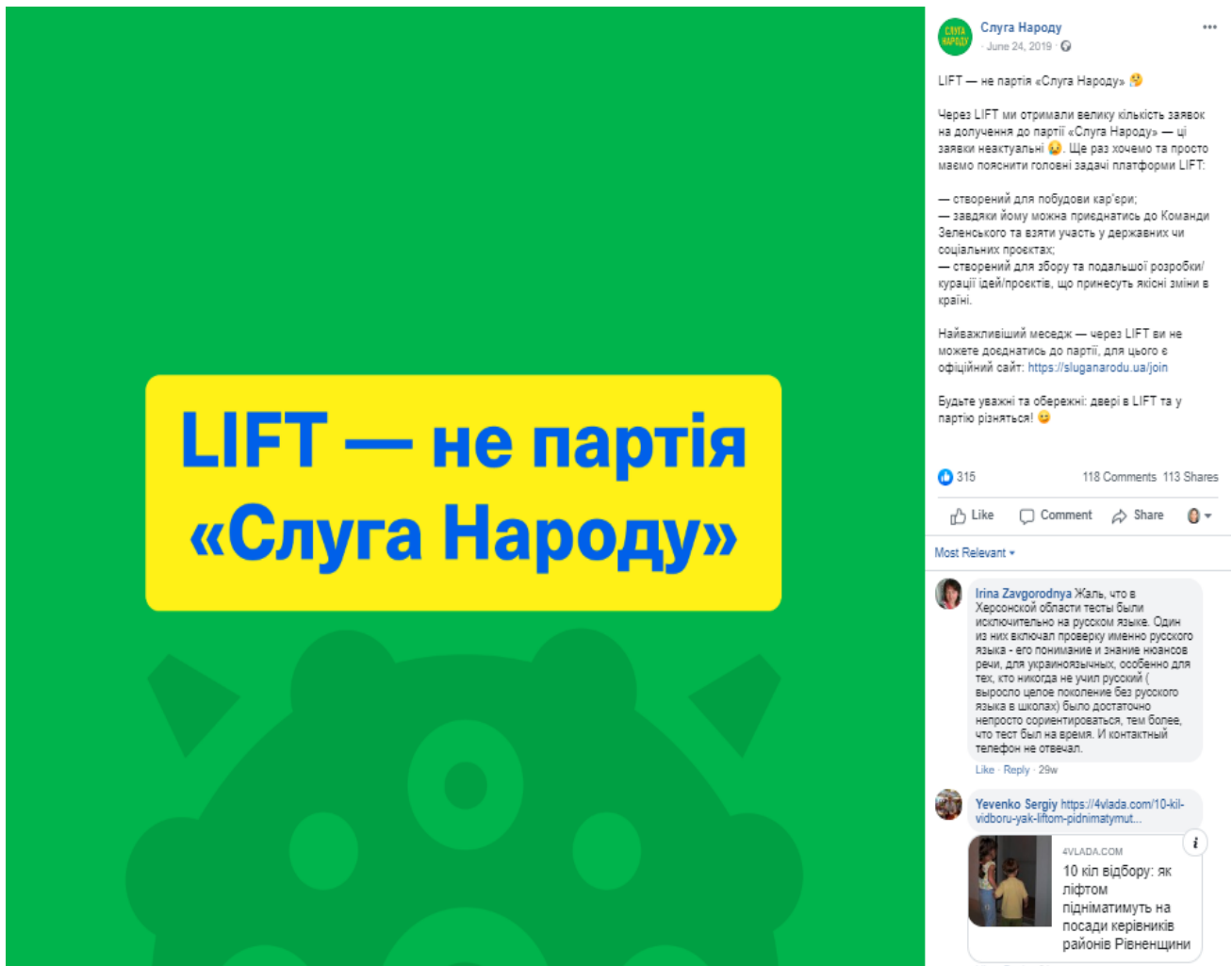
Як було вище зазначено в цьому дослідженні, деякі партії (такі, як “Слуга народу” або “Європейська солідарність”) спромоглися зібрати інформацію про десятки тисяч виборців онлайн та сегментувати її в досить деталізовані категорії згідно з демографічними чи поведінковими характеристиками. За словами консультанта з цифрового маркетингу, який працював на виборах 2019 року з політичними партіями, які ми розглядаємо в доповіді, значного базового списку потенційних виборців в поєднанні з можливостями таргетингу Facebook та Google завдяки таким функціям, як [“Lookalike Audiences”](#) Facebook, було б достатньо для того, щоб партія сформувала конкурентну цифрову кампанію в українських реаліях, навіть при тому, що дані користувачів цих платформ в Україні не такі деталізовані, як, наприклад, в США.

6. Міркування щодо володіння та обміну даними перед та після виборів

6.1. Партійні проекти

І перед, і під час виборів деякі партії запустили афілійовані проекти, спрямовані на збільшення кола активних громадян, які можуть розділяти партійні цілі, але не готові формально долучитися до лав політичної організації. Наприклад, декілька років тому “Європейська солідарність” розпочала спільний проект з IDF Reforms Lab та створила так званий Відкритий офіс, аби заохотити громадян, готових допомогти [“сформувати нову політичну культуру та імплементувати якісні реформи на всіх рівнях”](#). У 2019 році “Голос” запросив своїх найактивніших волонтерів та прихильників долучитися до Коворкінгу змін у декількох регіонах, а новообраний Президент України Володимир Зеленський оголосив про запуск “Ліфту” – проекту, спрямованого на залучення талановитих особистостей, які хотіли б втілити свої ідеї або вміння на користь [“позитивних змін в країні та її глибокого соціально-економічного і культурного розвитку”](#).

Проте, публікації на веб-сайті Відкритого офісу “Європейської солідарності” не демонструють жодної активності з 2018 року (навіть при тому, що там присутня працююча реєстраційна форма), а “Голос” використовував свої [регіональні коворкінги](#) для організації діяльності партійних волонтерів протягом кампанії. Натомість, стосунки між проектом “Ліфт” та “Слугою народу” були більш заплутані. [Опис на веб-сайті](#) свідчить, що цей проект є спробою новообраного Президента й уряду залучити кваліфікованих громадян на посади державних службовців та використати їхні ідеї для покращення державних послуг в ефективний і прозорий спосіб. Фактично, зараз користувачі можуть подати заявку на посаду в державному органі, за бажанням залишити заявку із загальною інформацією про себе та резюме або запропонувати механізм для оцифрування державних послуг. Хоча веб-сайт має політику конфіденційності та просить користувачів надати згоду на обробку даних, ніде не роз’яснюється точний зв’язок між платформою, партією та державними органами або тим, як проходить передача даних між проектом “Ліфт” і цими третіми сторонами (фактично, політика конфіденційності лише стверджує, що “адміністрація веб-сайту зв’яжеться з користувачем за потреби використання персональних даних для цілей, що не вказані в переліку”, який не включає, наприклад, передачу даних державним органам). Такий неясний зв’язок створив плутанину між прихильниками “Слуги” протягом періоду агітації, коли багато людей подавали заявки через веб-сайт для того, аби долучитися до лав партії, а потім виявляли, що їхні заявки були недейсними (Зображення 40). Водночас, під час активації платформи голова виборчого штабу партії “Слуга народу” натякав на те, що цей проект може застосовуватися і для пошуку кандидатів для участі у виборах.

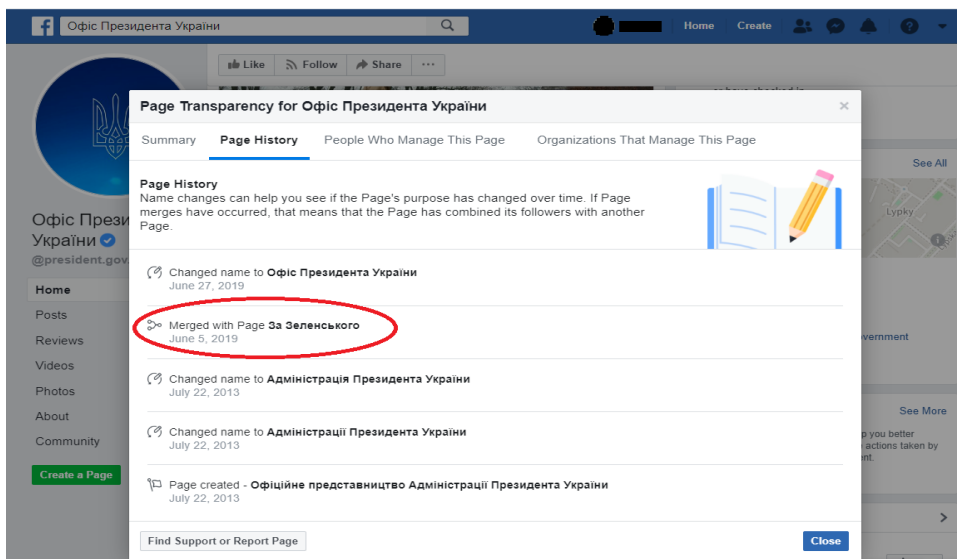


Зображення 40: 24 червня 2019 року, пост на сторінці “Слуги народу” у Facebook, яка пояснює, як саме долучитися до партії через веб-сайт, а не через “Ліфт”, скріншот від 19.03.2020.

6.2. Державні установи та народні обранці

Для партій та кандидатів, які виграють вибори, дані про виборців, зібрані під час кампанії, не втрачають ваги. Проте, партії в своєму новому статусі мають користуватися ними з особливою уважністю. Так, навіть якщо виборці дали згоду на те, щоб їхня інформація використовувалася партією або кандидатом після виборчого циклу, вони можуть не очікувати того, що їхні дані опиняться в руках державного службовця, будуть поширені або використані державним органом чи іншим політичним гравцем. Навіть якщо народні обранці технічно не володіють даними (наприклад, підписниками в соцмережі), але “успадковують” їх від партії, яка висунула їх в якості кандидатів, варто взяти до уваги ті самі застереження.

Наприклад, історія сторінки адміністрації президента України у Facebook демонструє, що після президентських виборів 2019 року нові адміністратори просто об’єднали її зі сторінкою прихильників Володимира Зеленського, залишивши [180 тис. підписників](#) без права вибору: чи хочуть вони підписниками сторінки Офісу Президента, чи ні.



Зображення 41: історія сторінки Facebook, що належить Офісу Президента, демонструє злиття з фан-сторінкою В.Зеленського після виборів, скріншот від 09.03.2020.

Крім цього, у листопаді 2019 року, засновник одного з провідних цифрових маркетингових агентств України [опублікував](#) скріншот електронного листа від новоствореного Міністерства цифрової трансформації, в якому стверджувалося, що він починає отримувати такі листи на одноразову електронну скриньку, спеціально створену ним раніше для того, щоб підписатися на розсилку від передвиборчої кампанії Володимира Зеленського (Зображення 42).



Зображення 42: пост у Facebook від 4.11.2019, в якому користувач скаржиться на отримання електронного листа від Міністерства на адресу, яку він надавав лише кампанії В. Зеленського, скріншот від 10.05.2020.

7. Висновки та рекомендації

Цією публікацією ми хочемо зробити внесок до все більшого обсягу досліджень про вплив технологій, що оперують персональними даними, на перебіг політичних кампаній. Для цього ми вивчили ставлення п'яти політичних партій до персональних даних виборців протягом парламентських виборів 2019 року в Україні. Щоб дати відповідь на важливі питання, які стосуються наслідків використання цих технологій для виборців, політичних суб'єктів, законодавців та демократичного процесу як такого, необхідно зрозуміти, як такі технології застосовуються в різних країнах та який рівень впливу на політичні процеси вони мають в різному політичному, правовому та соціальному контекстах. Таке дослідження особливо важливе в світлі швидкого розвитку технологій та зростання кількості шляхів застосування галузі комерційних даних для політичних цілей. Важливо, що до цих методів звертаються не лише традиційні політичні гравці, але й багато інших суб'єктів за межами виборчих циклів.

Виходячи з результатів цього дослідження, ми пропонуємо на розгляд **політичним партіям, законодавцям та громадянському суспільству** ряд важливих питань та рекомендацій. Ми сподіваємося, що наші висновки допоможуть стимулювати обговорення цих питань в Україні та надихнуть дослідників провести схожий аналіз в інших країнах.

- Стрімкий розвиток і поширення технологій, що використовують персональні дані для політичних цілей, створюють правовий вакуум, в якому нові інструменти масово використовуються в умовах ігнорування правових норм. Ця ситуація ускладнюється ще й тим, що суспільство не має можливості повністю усвідомити, до яких технологій звертаються політичні суб'єкти протягом кампанії і як далеко вони готові зайти. За таких обставин важливо, щоб політичні партії думали не тільки про відповідність правовим нормам, але й про формування своєї політичної практики в рамках етики. Також важливо серйозно обмірковувати та надавати повну інформацію про використання персональних даних виборців, включаючи надання доступу до них третім сторонам. Як мінімум, партії мають сформулювати чіткі та зрозумілі політики конфіденційності/захисту персональних даних, розмістити їх на своїх агітаційних платформах та переконатися в тому, щоб користувачі надавали згоду до того, як їх дані будуть зібрані. Рекомендується, щоб партії посилювали свої практики захисту персональних даних поясненням того, що саме вони роблять, щоб забезпечити захист персональних даних виборців.
- Партіям, які вже мають політики конфіденційності, варто визначитися, як саме відповідні принципи втілюються в життя на практиці з урахуванням різноманітності інструментів, які застосовуються для цифрової агітації, а також переконатися, що відповідні особи знають про ці директиви й що вони послідовно їх дотримуються на кожному рівні організаційної структури партії.
- Ми виявили, що питання безпеки партійних сайтів та інших онлайн-інструментів, які використовуються протягом виборчої кампанії, часто згадуються в останню чергу. Хоча не всі партії мають однакові ресурси під час кампанії, цей аспект має завжди бути пріоритетним, а належні заходи для захисту персональних даних виборців мають вживатися вчасно. Як показує приклад виборів в США у 2016 році, прогалина в системі безпеки може мати далекосяжні негативні наслідки не

лише для партії або виборців, якщо їхні дані було скомпрометовано, але впливати на результати виборів і навіть змусити суспільство сумніватися в легітимності виборчого процесу загалом.

- Інформація про виборців, яку збирають партії, не просто магічним чином не зникає після виборів, вона ще й не втрачає своєї цінності. Партії, які виграють вибори, мають дуже уважно ставитися до даних виборців, які вони зібрали. Коли виборці дають згоду на те, щоб їхні дані могли використовуватися після завершення виборчого циклу, вони не очікують на те, що дані опиняться в руках державного службовця або будуть поширені чи використані офіційним державним органом. Такого не має відбуватися автоматично, навіть у випадках, коли партія отримує беззаперечну підтримку населення та очолює процес формування уряду. Саме тому так важливо зробити процеси обробки та передачі даних після виборів максимально прозорими і зрозумілими для виборців, адже це може вплинути на рівень їхньої довіри до уряду та до політичної системи в цілому.
- Законодавці та керівництво ЦВК готові запроваджувати такі інновації, як електронне голосування, в той час, як чинному законодавству бракує важливих роз'яснень, механізмів та безпекових заходів, необхідних для регулювання цифрової агітації та захисту персональних даних виборців. Як мінімум, у законодавстві має бути визначено, що цифрові методи (враховуючи, але не обмежуючись політичною онлайн-рекламою) є офіційною формою проведення агітації. Слід також законодавчо врегулювати такі нагальні проблеми, як дискредитація та поширення дезінформації під час онлайн-агітації, роль сторінок, що офіційно не пов'язані з політичними кандидатами, або використання ботів та фейкових акаунтів. Окрім цього, ЦВК має забезпечити чіткий механізм фінансової звітності політичних партій і кандидатів в аспекті цифрової агітаційної діяльності, щоб створити основи для притягнення правопорушників до відповідальності.
- Жодні додаткові регулювання цифрової агітації (у випадку прийняття) не мають загрожувати свободі слова онлайн. Більше того, онлайн-платформи роблять суттєві кроки назустріч підвищенню прозорості та підзвітності цифрової політичної реклами і пристосовують свої практики до виборчого права. Україна має вживати заходів для координації своєї діяльності з технічними гігантами на міжнародному рівні, щоб переконатися в тому, що міжнародні компанії дотримуються її виборчого законодавства.
- Персональні дані, які стосуються політичних вподобань громадян та їхнього членства в політичних організаціях, вважаються за українським законодавством "чутливою" інформацією. Тому законодавство закликає до посилення безпекових заходів стосовно таких даних. У той час, як партії, які збирають інформацію про своїх членів, начебто звільняються від надання відповідних повідомлень до Секретаріату Уповноваженого, чинні норми не уточнюють, як саме треба поводитися з даними не-членів партій: волонтерів, прихильників та інших виборців, зібраних партіями та кандидатами під час виборчої кампанії. До того ж, викликає сумніви ефективність механізмів, що мають цей захист забезпечити, адже в Україні відсутній окремий орган із захисту даних з достатніми повноваженнями та ресурсами для забезпечення дотримання цих норм.

- Окрім цього, закон неявно вимагає від політичних партій переконатися в безпеці своїх веб-сайтів, аби захистити дані виборців від перехоплення чи втрати. Але роз'яснення про те, що включає в себе забезпечення такого захисту веб-сайту або іншого цифрового інструменту, відсутнє. І нехай подібні роз'яснення в законі краще будуть відсутні, але політичним партіям та іншим суб'єктам, задіяним в політичних кампаніях, не завадило б отримати чітке керівництво про захист персональних даних громадян, а також про ефективні механізми посилення цифрової безпеки. Громадянське суспільство могло б взяти на себе відповідальність за формулювання таких рекомендацій.

- Існує ще одна проблема, яка викликає навіть більше занепокоєння. Мова йде про відсутність культури приватності та слабку обізнаність про пов'язані з цим ризики серед громадян, приватних підприємств та органів державної влади. Обсяг персональних даних громадян, який вже доступний в мережі внаслідок витоків, хакерських атак або нелегальної торгівлі, створює серйозні ризики розповсюдження серед великої кількості громадян будь-якого потенційно шкідливого контенту. Ці персональні дані можуть бути використані як внутрішніми, так і зовнішніми суб'єктами в різноманітних контекстах, включаючи політичний. Перед обличчям такої загрози Україна має зробити посилення механізмів захисту даних своїм пріоритетом, а громадянське суспільство може працювати над підвищенням усвідомлення значущості приватності серед громадян.

- Водночас, поширення непрозорих та складних технологій, які застосовуються в політичній агітації, може приголомшувати виборців і поглиблювати відчуття маніпульованості та недовіри до політиків і уряду. Громадянське суспільство в Україні має розвивати цифрову обізнаність виборців та вимагати прозорості механізмів, що застосовуються для цифрової агітації таким чином, аби при цьому громадяни не втрачали довіри до політичних партій та виборчого процесу як такого.