Аналітична записка
Серія «Інформаційна стратегія», № 1, 2019

ВИБОРИ У ФРАНЦІЇ 2017 РОКУ: ВИСНОВКИ ДЛЯ УКРАЇНИ

А. В. Баровська, к. н. держ. упр., заступник завідувача відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень

У 2017 році Франція пройшла через дві загальнонаціональні виборчі кампанії – президентську та парламентську. Обидві були визнані незалежними спостерігачами надзвичайно захищеними від зовнішнього втручання. Для цього уряд Франції вжив низку заходів. Цей досвід варто адаптувати для потреб поліпшення захисту українського виборчого процесу.

ВИСНОВКИ

1. Досвід захисту виборчого процесу у Франції в 2017 році виявився ефективним і може бути використаний для поліпшення захисту виборчого процесу в Україні.

2. Основна новація виборчого циклу 2017 року – активна діяльність Національної агенції з безпеки інформаційних систем (*ANSSI*), яка займалась

кібербезпекою не лише виборчої системи, але й учасників виборчого процесу.

3. Було **продовжено практику 2012 року щодо моніторингу соціальних мереж** під час виборчої кампанії, зокрема, на предмет виявлення маніпулювання громадською думкою (здійснювала Національна комісія з контролю за виборчою кампанією за підтримки Міністерства внутрішніх справ) – це дозволило вчасно виявляти факти дезінформації.

4. Для зменшення вірогідності маніпуляцій **Франція відмовилась від електронного голосування на користь паперового** (у т.ч. для французьких громадян за кордоном). Рішення було ухвалене за результатом проведення декількох хвиль аудиту ІТ-систем, задіяних у виборчому процесі.

5. Напередодні виборів Національна комісія з контролю за виборчою кампанією створила **протокол для реагування на масштабну кібератаку**. Його використали під час «*Macron Leaks*» і він довів свою ефективність.

6. Для зменшення впливу маніпулятивної інформації **було також вдосконалено законодавство**, а перші особи публічно підкреслювали, що готові захищати демократію від маніпуляцій.

РЕКОМЕНДАЦІЇ (ЦВК)

1. **Провести** за результатами двох виборчих кампаній 2019 року **комплексну оцінку щодо виявлених під час виборів фактів зовнішнього втручання у виборчий процес та вжитих у відповідь заходів**. Для проведення оцінки залучити, як урядові так і недержавні структури.

2. Провести серію круглих столів та закритих обговорень із зацікавленими сторонами (стейкхолдерами) щодо **вдосконалення механізмів протидії фейкам та маніпулюванню громадською думкою у виборчий період**.

3. Проаналізувати доцільність **розширення спроможностей ЦВК в частині вчасного виявлення поширення в них фейкової інформації**, що може істотно вплинути на виборчий процес.

4. **Посилити співпрацю ЦВК з ключовими соціальними мережами** (передусім – *Facebook, Instagram, YouTube, Twitter*):

- встановити з ними офіційні контакти та підписати **спільні меморандуми** про напрямки взаємодії під час виборчого періоду;

- **обмінюватись даними** щодо політичної реклами під час виборів (для недопущення порушення «дня тиші» чи уникнення обмежень законодавства в частині видатків на політичну рекламу);

- **доводити до представників соціальних мереж факти поширення на їх**

платформах фальшивої інформації з метою подальшого використання алгоритмів сервісів для припинення цього процесу.

5. Розробити **план комунікування кіберінцидентів** (у т.ч. визначити часові проміжки реагування, механізми міжвідомчого вироблення спільних меседжів, цільові аудиторії, канали, процедури, попередню підготовку повідомлень тощо).

6. Спільно з іншими урядовими та неурядовими структурами напередодні виборів **проводити кампанії з підвищення обізнаності з кібербезпеки,** як для широкої громадськості так і для учасників політичних кампаній (в т.ч. кандидатам в президенти України, політичним партіям та кандидатам в народні депутати). Спільно з Національним координаційним центром кібербезпеки при РНБО:

- **сформувати перелік експертів з кібербезпеки** (зокрема з числа неурядових фахівців), які могли б консультувати учасників виборів з питань кібербезпеки їх інформаційних ресурсів;

- **розробити інструкції** (методичні рекомендації, керівництва тощо) з питань забезпечення кібербезпеки.

Франція є однією з країн, які нещодавно проходили крізь дві виборчі кампанії - президентську, що завершилась 7 травня 2017 року, та парламентські вибори, що відбулись 18 червня 2017 року. За оцінками експертів, під час обох вона змогла належним чином протидіяти сторонньому впливу.

Підготовка Франції до процесу виборів і убезпечення їх від сторонніх втручань може бути умовно поділена на два періоди:

- довиборчий (підготовка законодавства);

- безпосередньо під час виборів (заходи з недопущення кібервтручань та використання соціальних мереж для поширення фейків / дезінформації).

На довиборчому етапі було ухвалено закон, спрямований на зміцнення свободи, незалежності та плюралізму ЗМІ (*Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias*). Закон вимагає від засобів масової інформації **прийняття кодексу етики та створення комітету з етики** для полегшення вирішення внутрішніх суперечок, а також конфліктів між редакціями газет та власниками ЗМІ.

З метою забезпечення фізичної безпеки президентських та парламентських виборів у Франції було впроваджено план *Vigipirate*[1] та продовжено надзвичайний стан, що його раніше введено у країні[2]. Причому, вводячи в дію надзвичайний стан

[1] *Plan Vigipirate* – це національна система Франції щодо оповіщення про рівень терористичної загрози. Вона була створена у 1978 році та з того часу декілька разів оновлювалась.

[2] Спочатку надзвичайний стан був введений президентом Франсуа Олландом відразу після терактів у Парижі 13 листопада 2015 року. Після теракту у Ніцці в липні 2016 року, Національна асамблея продовжила надзвичайний стан ще на шість місяців, до кінця січня 2017 року.

у 2015 році, Національна асамблея скасувала положення Закону про надзвичайний стан 1955 року (*Loi relative à l'état d'urgence*), що дозволяли контролювати медіа-контент та здійснювати адміністративні обшуки у редакціях. Як згодом відзначали експерти спостережної місії ОБСЄ, надзвичайний стан не позначився на кліматі виборчої кампанії та проведені голосування.

Під час виборів основний акцент було зроблено на безпеку інформаційних систем, що використовувались у процесі виборів – вони стали предметом аудиту *ANSSI (Національна агенція з безпеки інформаційних систем – Agence nationale de la sécurité des systèmes d'information),* який дозволив визначити потенційні ризики. Задля гарантування безпеки інформаційних систем урядом Франції було здійснено такі кроки:

- подовжено мораторій на використання машин для голосування на виборчих дільницях (діє з 2007 року);

- відмова від голосування через інтернет для французьких громадян за кордоном[3] під час парламентських виборів. Рішення було ухвалене урядом на основі зроблених *ANSSI* зауважень – на їх думку, надзвичайно високий рівень загрози кібератак міг вплинути на проведення електронного голосування;

- налагоджено взаємодію з Міністерством внутрішніх справ для убезпечення інфраструктури, яка використовуватиметься для передачі результатів виборів з виборчих дільниць.

ANSSI вирішило і ще одне завдання, розширило коло об'єктів захисту за рахунок суб'єктів політичного процесу. У Франції, як і у США, комп'ютерна безпека партій є найбільш слабкою ланкою виборчого процесу, відтак було ухвалене рішення, що *ANSSI* має надавати консультативну та експертну допомогу з питань кіберзахисту кандидатам та політичним партіям. 26 жовтня 2016 року, напередодні виборчих перегонів, представників усіх партій та рухів Франції було запрошено на спеціальний семінар з кібербезпеки. Єдиною політсилою, що проігнорувала семінар, став Національний фронт Марін Ле Пен (*Marine Le Pen*). На семінарі *ANSSI* повідомила політичні партії та кандидатів, що вони готові провести аудит безпеки та запропонувати рішення з удосконалення захисту комп'ютерів та інтернет-ресурсів від кібератак. Також *ANSSI*:

- передала присутнім на семінарі перелік сертифікованих незалежних експертів, які могли б обстежити та протестувати їх кіберінфраструктуру;

[3] Електронне голосування було запроваджено у Франції у 2012 році, але тільки для парламентських виборів і тільки для виборців, що зареєстровані в одному з 11 виборчих округів за кордоном, а також для виборів радників консульств. // Législatives : pas de vote électronique pour les Français de l'étranger. – https://www.lesechos.fr/2017/03/legislatives-pas-de-vote-electronique-pour-les-francais-de-letranger-164704

- надала працівникам, залученим до проведення виборчих кампанії, інструменти для моніторингу та виявлення підозрілої активності в інформаційних системах кандидатів (зокрема, *DOS* або *DDoS* атак, незвичної активності та вторгнення), у т.ч. 36-сторінкове керівництво з кібербезпеки та підручник щодо DDoS-атак на 52 сторінках.

Також було вжито низку заходів з попередження втручання у виборчий процес, що пов'язані з недопущенням поширення фейків / дезінформації (особливо в соціальних мережах). Моніторинг мереж здійснювався Національною комісією з контролю за виборчою кампанією (*Commission Nationale de Controle de la Campagne Electorale*, скор. *CNCCEP*) за підтримки Міністерства внутрішніх справ (надало відповідну експертну групу). Метою моніторингу було збільшення поінформованості *CNCCEP* про будь-які відхилення ситуації від нормальної, вимірювання масштабів проблеми та, за необхідності, публічне втручання. Моніторингова група:

- оцінювала «вірусність» можливих фальшивих новин (fausses nouvelles) та здійснювала їх юридичну кваліфікацію;

- готувала щоденний звіт на основі аналізу повідомлень публічного характеру (проте вона не відслідковувала приватну кореспонденцію).

Кейс «*Macron Leaks*»[4] довів, що вжиті урядом заходи та загальна увага суб'єктів виборчого процесу до власної кібербезпеки була недаремною. Водночас ефективність контрдій була обумовлена не лише завчасними організаційними та технічними заходами безпеки, але й ефективною та швидкою комунікацією всіх державних структур під час цієї атаки.

Ключову роль у забезпеченні безпеки президентських виборів 2017 року у Франції відігравали Національна комісія з контролю за проведенням виборчої кампанії та Національна агенція з безпеки інформаційних систем. Ці установи, на думку експертів, діяли ефективніше, ніж американські, у т.ч. завдяки централізованому підходу (у США таку діяльність федеральні установи мають координувати з відповідними органами на рівні штату, а підходи на рівні штатів можуть відрізнятися).

З урахуванням набутого протягом проведення двох загальнонаціональних кампаній 2017 року досвіду в листопаді 2018 року було ухвалено «Закон щодо протидії маніпулюванню інформацією» («*contre la manipulation de l'information»*). Метою закону є адаптація правових інструментів для боротьби з неправдивими новинами до середовища, в якому функціонують такі нові засоби доставки та поширення, як:

[4] Інцидент з витоком вкраденого електронного листування команди Е. Макрона – 9 гігабайтів фалів та 21 тис. електронних листів, що з'явилися на декількох інтернет-сайтах у п'ятницю 5 травня 2017 року пізно ввечері.

- медіа, що контролюються іноземними державами;

- цифрові платформи, що ховаються за своїм статусом «провайдера хостинга контенту», щоб не брати на себе відповідальність за контент, який вони транслюють.

Серед важливих норм закону:

- вимога прозорості цифрових платформ (передусім – соціальних мереж), що матимуть повідомляти про спонсорований контент, публікуючи ім'я автора та сплачену суму. Також платформи мають надавати інформацію про використання персональних даних. Порушення цих зобов'язань карається одним роком тюремного ув'язнення та штрафом у розмірі 75 тис. євро;

- Вища рада з аудіовізуальних питань (*le Conseil supérieur de l'audiovisuel*) отримала повноваження запобігати, призупиняти або переривати мовлення телевізійних служб, що контролюються іноземною державою або перебувають під її впливом, якщо вони поширюють фальшиві новини з метою впливу на результати голосування;

- процедура розгляду судового позову в пришвидшеному порядку, щоб мати можливість оперативно зупиняти поширення фальшивих новин (рішення має бути ухвалене протягом 48 годин). Саме суддя має кваліфікувати «фальшиві новини» згідно з визначенням закону 1881 року за трьома критеріями: очевидність[5]; масове та штучне поширення; порушення громадського спокою або вплив на свідомий вибір.

[5] За формулюванням статті вказаного Закону.