ДК 343.415

Тетяна Петрівна Матюшкова,

кандидат юридичних наук, доцент,

доцент кафедри криміналістики та судової експертології

Харківського національного університет внутрішніх справ

Використання інформаційних технологій при вчиненні окремих видів злочинів проти виборчих прав громадян

Компанія Google, Facebook та Twitter заявили про використання своїх серверів для розповсюдження дезінформації під час передвиборчої кампанії президента США, що могло суттєвим чином вплинути на результати виборів. За повідомленнями у засобах масової інформації, на 1 листопада цього року у Конгресі США заплановані слухання відносно незаконного втручання у вибори, у зв'язку з чим представники зазначених кампаній викликані для дачі показань [1]. Про вплив ботів і фейків на вибори у Німеччині свідчать дослідження Оксфордського університету [2].

Використання інформаційних технологій при вчиненні злочинів проти виборчих прав громадян має місце й в Україні. Так, за період чергових місцевих виборів 2015 року Національною поліцією було розпочато 478 досудових розслідувань за статтями 157-160 Кримінального кодексу України (далі – КК України), якими встановлюється відповідальність за злочини проти виборчих прав громадян. Майже 16% з яких (78 кримінальних проваджень) стосувались, зокрема, надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (ст. 158 КК України). [3].

Зазначені злочини можуть бути вчинені такими способами, визначеними у диспозиції ст. 158 КК України: 1) умисне подання до органу ведення Державного реєстру виборців неправдивих відомостей про виборців; 2) умисне внесення неправдивих відомостей до бази даних Державного реєстру виборців; 3) несанкціоновані дії з інформацією, що міститься в базі даних Державного

реєстру виборців; 4) інше несанкціоноване втручання у роботу бази даних Державного реєстру виборців. Саме останні три способи пов'язані з використанням інформаційних технологій.

Як свідчать матеріали слідчої і судової практики й результати інтерв'ювання спеціалістів у галузі інформаційних технологій, несанкціоноване втручання у роботу бази даних Державного реєстру виборців здійснюється, наприклад, за рахунок DDoS-атаки на сайт Центральної виборчої кампанії (далі – ЦВК). Такий вплив здійснюється з метою:

1) зашкодити нормальній роботі сайту через його перевантаження щоб блокувати доступ користувачів до сайту та розміщених на ньому даних (DDoS-атака як кінцева мета, щоб викликати панічні настрої, недовіру населення до результатів виборів в цілому чи на окремих виборчих дільницях);

2) виявити уразливості у інформаційній безпеці та завантажити шкідливе програмне забезпечення (далі – ШПЗ), використання якого дозволить зловмисникам в подальшому внести неправдиві відомості, порушити встановлений порядок маршрутизації інформації, вчинити інші несанкціоновані дії (DDoS-атака як прикриття подальших злочинних дій проти виборчих прав громадян);

3) отримати доступ до супутніх серверів, якими здійснюється певний вид операцій, результати яких відображаються на офіційному сайті ЦВК. Незаконний доступ дозволяє зловмисникам безпосередньо внести неправдиві відомості до Державного реєстру виборців, підробити інформацію про хід і результати волевиявлення на окремих виборчих дільницях, спотворити процес її обробки, чим сфальсифікувати підсумки голосування (DDoS-атака як засіб отримати несанкціонований доступ та підробити результати голосування).

Зазначені технології реалізуються, як правило, так званими «зовнішніми» суб'єктами, тобто особами, які не пов'язані трудовими відносинами із підприємством, установою чи організацією, на ресурси яких здійснюється незаконний вплив з використанням інформаційних технологій, у тому числі, й при активному використанні ними бот-нетів. Разом з тим, несанкціоноване

втручання у роботу бази даних Державного реєстру виборців, сайту Центральної виборчої кампанії й супутніх серверів може здійснюватись і так званим «внутрішнім» суб'єктом:

1) співробітником ЦВК чи її структурних підрозділів –

   а) відділу адміністрування та інформаційної безпеки, інформаційного забезпечення, аналітичної обробки інформації чи(і) супроводу програмного забезпечення Управління інформатизації Секретаріату ЦВК;

   б) відділів ведення Державного реєстру виборців, які уповноважені здійснювати дії щодо ведення Реєстру виборців, використовувати засоби програмного забезпечення автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців» [4];

2) співробітником підприємства, установи, організації, що здійснює загальносистемне програмне забезпечення для функціонування автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців» [6].

Використання інформаційних технологій при фальсифікації підсумків голосування або відомостей Державного реєстру виборців зазначеними суб'єктами полягає у безпосередньому завантаженні ними шкідливого програмного забезпечення шляхом під'єднання зовнішніх носіїв інформації, заражених ШПЗ, відкриття електронного листа чи переходу за посиланням на сайт, що містить ШПЗ, ін. Зазначені дії можуть бути здійснені заздалегідь і наявне ШПЗ спрацьовує у потрібний зловмисникам час, що дозволяє їм непомітно подолати систему безпеки, несанкціоноване втрутитись у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, спотворити процес обробки, підробити або порушити встановлений порядок маршрутизації інформації про хід та результати волевиявлення громадян на виборах.

Використання інформаційних технологій може мати місце й при вчиненні інших злочинів проти виборчих прав громадян. При перешкоджанні

здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача, поєднаному із примушуванням, використання інформаційних технологій може полягати у створенні спам-розсилок із погрозами на адресу конкретних осіб. При підкупі виборця, учасника референдуму, використання інформаційних технологій полягатиме у здійсненні безготівкових розрахунків. При порушенні порядку фінансування політичної партії, передвиборної агітації, агітації з всеукраїнського або місцевого референдуму, використання інформаційних технологій полягатиме у розміщені на сайтах різних відомих провайдерів, громадських організацій, політичних партій, засобів масової інформації спеціальних політичних рекламних оголошень, пропагандистських текстів і політичних новин на користь конкретного кандидата, чи(і) неправдивих інформаційних повідомлень, спрямованих на дискредитацію окремих кандидатів, у тому числі, через мережу спеціально створених чи придбаних облікових записів, шляхом активного використання бот-мереж, інструментів інтернет-троллінгу, посилань на сторонні ресурси, ін.

Резюмуючи вищевикладене слід відзначити, що використання інформаційних технологій набуває широкого розповсюдження при вчиненні злочинів проти виборчих прав громадян у всьому світі, що вимагає подальших ґрунтовних досліджень у цьому напрямку з метою розробки ефективної методики їх виявлення, розслідування та запобігання.

Список використаних джерел:

1. Facebook, Google и Twitter выступят перед Конгрессом по делу о вмешательстве России в выборы в США [Електронний ресурс] / Режим доступу : https://itc.ua/news/facebook-google-i-twitter-vyistupyat-pered-kongressom-po-delu-o-vmeshatelstve-rossii-v-vyiboryi-v-ssha/ **2.** Боти і фейки впливають на вибори в Німеччині менше, ніж впливали у США – дослідження [Електронний ресурс] / Режим доступу : http://gordonua.com/ukr/news/politics/-boti-i-fejki-vplivajut-na-vibori-v-nimechchini-menshe-nizh-vplivali-v-ssha-doslidzhennja-208210.html

3. Дайджест №1. Розслідування виборчих злочинів на чергових місцевих

виборах в Україні 2015 року: статистика і попередні висновки [Електронний ресурс] // режим доступу : https://www.oporaua.org/vybory/43146-opora-pidhotuvala-daidzhest-shchodo-rozsliduvannia-vyborchykh-zlochyniv-na-cherhovykh-mistsevykh-vyborakh-2015-roku **4.** Про Порядок організаційно-правової підготовки і виконання дій щодо ведення Державного реєстру виборців : Постанова Центральної виборчої комісії від 20 січня 2011 року № 13 [Електронний ресурс] // режим доступу : http://zakon2.rada.gov.ua/laws/show/en/v0013359-11

5. https://prozorro.gov.ua/en/tender/UA-2017-07-20-000127-c

Одержано ___.___.2017