УДК 343.415

Тетяна Петрівна МАТЮШКОВА,
кандидат юридичних наук, доцент,доцент кафедри
криміналістики та судової експертології факультету № 1
Харківського національного університет внутрішніх справ;
ORCID: http://orcid.org/0000-0001-7973-4581

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 та інш.

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 бібліографічних посилань: 1. Facebook, Google и Twitter выступят перед Конгрессом по делу о вмешательстве России в выборы в США // ITCua: сайт. URL: https://itc.ua/news/facebook-google-i-twitter-vyistupyat-pered-kongressom-po-delu-o-vmeshatelstve-rossii-v-vyiboryi-v-ssha (дата звернення: 03.10.2017). **2.** Боти і фейки впливають на вибори в Німеччині менше, ніж впливали у США – дослідження // Гордон: сайт. URL: http://gordonua.com/ukr/news/politics/-boti-i-fejki-vplivajut-na-vibori-v-nimechchini-menshe-nizh-vplivali-v-ssha-doslidzhennja-208210.html (дата звернення: 03.10.2017). **3.** ОПОРА підготувала дайджест щодо розслідування виборчих злочинів на чергових місцевих виборах 2015 року // ОПОРА: сайт. URL: https://www.oporaua.org/vybory/43146-opora-pidhotuvala-daidzhest-shchodo-rozsliduvannia-vyborchykh-zlochyniv-na-cherhov

ykh-mistsevykh-vyborakh-2015-roku (дата звернення: 03.10.2017). **4.** Про Порядок організаційно-правової підготовки і виконання дій щодо ведення Державного реєстру виборців: постанова Центральної виборчої комісії від 20 січ. 2011 р. № 13 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/en/v0013359-11 (дата звернення: 03.10.2017). **5.** Ліцензії на загальносистемне програмне забезпечення для функціонування автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців (на яке майнові права не передаються) // Prozorro: сайт. URL: https://prozorro.gov.ua/en/tender/UA-2017-07-20-000127-c (дата звернення: 03.10.2017).

Одержано 08.10.2017

УДК 343.98

Катерина Геннадіївна НЕЖЕВЕЛО,
курсант 4 курсу факультету № 1
Харківського національного університету внутрішніх справ;
Юлія Василівна ЗАБОЛОТНА,
кандидат юридичних наук, викладач кафедри криміналістики
та судової експертології факультету № 1
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0001-8854-8537

ШАХРАЙСЬКІ СХЕМИ, ПОВ'ЯЗАНІ З ОРЕНДОЮ ЖИТЛА

Незважаючи на те, що злочини у сфері шахрайства займають досить незначне місце (2–3 %), проте боротьба з цим видом злочинів є досить актуальною проблемою для правоохоронних органів. Це можна пояснити тим, що шахрайство має високу латентність – далеко не кожна постраждала особа заявить про вчинені шахрайські дії щодо неї,тим самим приховуючи злочин.

Відповідно до чинного кримінального законодавства шахрайство – це заволодіння чужим майном, або правом на нього шляхом обману або зловживання довірою (ч. 1 ст. 190 КК України). Пленум Верховного Суду України у постанові «Про судову практику в справах про корисливі злочини протии приватної власності» від 25.12.1992 р. (з наступними змінами) зазначив, що правоохоронним органам і судам слід мати на увазі, що обман (повідомлення потерпілому неправдивих відомостей або приховування певних обставин) чи зловживання довір'ям (недобросовісне використання довір'я з боку потерпілого) при шахрайстві застосовуються винною особою з метою викликати у потерпілого впевненість про вигідність або обов'язковість передачі йому майна чи права на нього .Існують певні типові шахрайські схеми, знання яких зменшить шанс обману:

1. При зверненні в ріелторські контори необхідно пам'ятати, що серед них дуже уміло і непомітно навчилися маскуватися так звані інформаційні агентства. Специфіка роботи цих організацій полягає в тому, що вони просто надають інформацію за запитом орендодавця або орендаря, до якої неможливо підібратися з боку закону, адже клієнт підписує договір, в якому дрібним шрифтом вказаний пункт про надання інформації. Власне в цьому і полягає суть послуги, за яку стягується плата. Причому, все або велика частина з цих адрес і телефонних номерів можуть виявитися «липовими». Обман, в основному, розрахований на приїжджих, довірливих і не занадто обізнаних людей.

2. Розраховано на орендодавця і полягає в наступному: людина знімає квартиру, як правило, на дуже нетривалий час, потім, представляючись агентом по оренді нерухомості, приводить в цю квартиру одного за іншим потенційних квартиронаймачів, а його повноваження підтверджує співучасник, що виступає в ролі власника цього житла. Кожен з тих, що погодилися зняти цю нерухомість платить, як кажуть, за потрійним тарифом: за послуги ріелтора, запоруку і ціну за місяць проживання. Після такої театральної вистави шахраї зникають, а обдурені орендарі починають один за іншим стягуватися до дверей нещасливої квартири, в яку потрапити вони не можуть, адже всім на руки були видані ключі від абсолютно інших замків.