УДК 342.951
DOI https://doi.org/10.32841/2307-1745.2023.64.21

Гуржій С. В.,
старший науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ТА КРИМІНАЛЬНО-ПРАВОВІ ОСНОВИ ПРОТИДІЇ РОСІЙСЬКИМ БОТАМ В УМОВАХ ВІЙНИ

Анотація. Стаття присвячена дослідженню проблематики поширенню у соціальних мережах ботів російського походження та виробленню ефективних засобів запобігання таким проявам. Визначено тенденції розповсюдження рф фейкових акаунтів та ботів з метою маніпулювання свідомістю, поширення антиукраїнських наративів, викрадення персональних даних та конфіденційної інформації. Окреслено загрози використання російських ботів у соціально орієнтованих ресурсах мережі Інтернет з метою здійснення деструктивної та підривної інформаційної діяльності на шкоду національним інтересам України. Розкрито поняття, зміст та особливості діяльності ботів у соціальних мережах. Акцентовано, що в сучасному світі боти генерують майже половину інтернет-трафіку світу. Визначено роль та місце ботів під час їхнього використання зловмисниками з метою поширення шкідливого програмного забезпечення. Розглянуто механізми використання ботів під час інформаційної війни рф проти України та визначено цілі й завдання російських глобальних інформаційних кампаній впливу. Деталізовано методи роботи російських спецслужб щодо нарощування зусиль із використання такого інструменту інформаційної війни як створення на платформах соціальних мереж «Facebook», «Instagram» і «Twitter» облікових записів (акаунтів), які містять недостовірні дані щодо користувачів, з метою проведення акцій інформаційного деструктивного впливу. Визначено засади політики конфіденційності таких сервісів як «Facebook», «Instagram» і «Twitter» стосовно використання підроблених облікових записів під час проведення реєстрації у якості ідентифікуючих даних інших осіб. Розглянуто ризики використання в Україні соціальної мережі «Telegram». Визначено передумови, ризики та загрози фішингу під час використання соціальною мережею «Telegram». Вказано роль фактчекінгу та кібергігієни як важливих складових профілатики виявлення, блокування та знищення російських ботів. Обгрунтовано актуальність застосування процедури клоакінгу з метою посилення захисту контенту від зовнішнього копіювання, шпигунських сервісів та шкідливих ботів. Узагальнено подальші шляхи удосконалення чинного законодавства з метою обмеження використання мережі «Telegram» в Україні. Визначено напрямки розробки дієвих механізмів протидії інформаційним атакам з використанням, на замовлення спецслужб рф ботів, які загрожують національній безпеці України. Розкрито європейський досвід законодавчого забезпечення боротьби з дезінформацією та нелегальним контентом у соціальних мережах та відомих інтернет-сервісах. На підставі узагальнення проведеного дослідження визначено організаційно-технічні основи та кримінально-правові засади запобігання деструктивній діяльності російських ботів в соціальних мережах та у всесвітній глобальній мережі.

Ключові слова: акаунт, бот, національні інтереси, війна, контент, соціальні мережі, фактчекінг, кібергігієна, клоакінг, фішинг.

Постановка проблеми. Держава-агресор – сучасна масшабна світова загроза на перманентній основі. В умовах триваючої війни рф проти України московія використовує усі наявні у своєму аресеналі сили та засоби з метою досягнення своїх амібтних цілей – захоплення територій та повалення конституційного ладу України. Важливе місце у сфері російської інформаційної експансійної політики у соціальних мережах посідають боти з метою їхнього злочинного використання на шкоду державним інтересам України та підриву міжнародного авторитету нашої країни. Російська Федерація, її спеціальні служби протягом тривалого часу проводять свої спеціальні інформаційні операції, більшість з яких спрямовані на ліквідацію української державності та знищення української ідентичності. Відбувається провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні з використанням саме деструктивного контенту [1, с. 168]. Досить успішно держава-агресор вдається до використання фейкових онлайн-акаунтів у соціальних мережах. За допомогою фейкових сторінок користувачів поширюються наративи «руського миру», спрямовані на дестабілізацію суспільно-політичної ситуації, відбувається маніпулювання свідомістю пересічних громадян, проводяться заходи з метою виманювання або викрадення персональних даних тощо. Паралельно росія активізує свій вплив на світову спільноту за допомогою ботів у вигідному пропагандистському руслі не тільки в Україні, але й навколо світу, в державах ЄС та США. Останнім часом виявлено чимало випадків та фактів активного використання російських ботів у соціально орієнтованих ресурсах мережі Інтернет з метою здійснення деструктивної та підривної інформаційної діяльності на шкоду державним інтересам, провокування витоку даних, крадіжок службової інформації. Такий стан справ вимагає ефективного реагування на чисельні прояви злочинної діяльності російських спецслужб за допомогою ботів у мережі Інтернет з метою їхнього виявлення, блокування та знищення. В умовах війни це важливі кроки, спрямовані на запобігання деструктивній інформаційній експансії рф. Саме тому висвітлення питань щодо організаційно-технічних основ та кримінально-правових механізмів запобігання деструктивній діяльності російських ботів в соціальних мережах є тематично актуальним та заслуговує на увагу.

Результати аналізу останніх досліджень і публікацій. Питання поширення фейкових облікових записів у соціальних мережах досліджували у своїх працях: О.Войтович, Л. Куперштейн, В. Головенко [2]. Актуальні проблеми протидії інформаційним загрозам у соціальних медіа під час повномасштабного вторгнення рф в Україну вивчали: О. Кантур [3], Л. Котихова [4], О. Левін [5], О. Панченко [6], О. Поляков [7]. Проблематика загрозливого використання ботоферм на шкоду державним інтересам перебувала у фокусі уваги таких науковців, як: Т. Лиска та В. Паламарчука [8], А. Юшкова [9]. Проте вказані фахівці не акцентували достатньої уваги на питаннях створення механізмів боротьби з масовим поширенням фальсифікованих акаунтів та ботів російського походження, предметно не визначали напрями удосконалення чинного законодавства щодо посилення заходів кримінально-правового впливу у цій площині.

Метою статті є узагальнення тенденційного використання та масштабів глобального поширення російських ботів як складової інформаційно-психологічних операцій кремля, особливо в умовах тотальної війни. Визначення організаційно-технічних основ та кримінально-правових засад з метою удосконалення системи реагування на випадки злочинного використання ботів у соціальних мережах та у всесвітній глобальній мережі.

Виклад основного матеріалу. Оскільки середній користувач Інтернету витрачає понад двох годин на день у соціальних мережах, Інтернет став чи не провідним місцем для спілкування про події, культуру та політику, підвищуючи важливість впливу на те, що бачать і говорять у мережі. На цьому фоні фейкові акаунти або боти існують у кожній соціальній мережі та їх налічується мільйони. Боти являють собою автоматизовані облікові записи в соціальних мережах, запрограмовані на певні дії, що імітують поведінку реальних Інтернет-користувачів. Сукупність таких облікових записів, запрограмованих на однакові дії та об'єднаних спільною метою, утворюють мережу ботів (ботнет), що характеризується наявністю великої кількості зв'язків у формі взаємної підписки на інші акаунти для відслідковування розміщення в них контенту та інших видів взаємодії.

Тобто боти – це спеціальні програми, які виконують автоматично або за заданим розкладом певні дії через ті ж інтерфейси, що й звичайні користувачі. Бот може виглядати як звичайний користувач мережі зі своїм профілем у соціальних мережах, ставити вподобайки й писати коментарі, публікувати дописи у фейсбуці, вайбер- і телеграм-групах, ютубі тощо. Боти можуть виконувати практично будь-які завдання, зокрема розважати, шукати, транслювати, переглядати, «лайкати», підписувати та публікувати контент. За своїм змістом, боти – це зручний для людини інтерфейс роботи із різноманітними веб-службами. Саме тому боти технологічно продовжуватимуть динамічно розвиватися, щоб краще імітувати людську поведінку, головним чином завдяки впровадженню штучного інтелекту. З виникненням штучного інтелекту можна згенерувати тисячі якісних фото людей, яких насправді не існує. Боти на основі штучного інтелекту здатні розпізнавати людську мову, аналізувати повідомлення, виявляти потреби користувача. Навіть отримало поширення програмне забезпечення – так звані «бот-комбайни», яке дозволяє керувати десятками та сотнями таких акаунтів. Це настільки продумана технологія, що роботи-адміністратори соціальних мереж не завжди можуть відрізнити фейки від реальних користувачів. Типовими ознаками бота є такі характеристики: – обліковий запис з низьким рівнем активності; – стандартний або повторюваний контент; – використання відповідей з певними ключовими словами; – велика кількість підписників без активності.

В сучасному світі боти генерують майже половину інтернет-трафіку світу. Так у 2019 році люди власноруч генерували 68,2% усього трафіку мережі, у 2021 році – 57,7% людської присутності в інтернет-трафіку, а у 2022 році лише 52,6%, а відтоді цей показник неухильно знижується [10]. Боти, як спеціальне програмне забезпечення здебільшого не займається створенням контенту, а виконує інші цілі – стеження, збір даних, аналіз тощо. Зазвичай ботів поділяють на «поганих» і «нейтральних», тому що «добрих» не існує за визначенням. У кращому разі від дій бота не буде прямої шкоди, але він все одно споживає ресурси й створює перешкоди в роботі сайтів, коли моніторить їхню активність або веде індексацію контенту. Так, наприклад, у 2022 році 51,2% усіх ботів належали до категорії «поганих» і мали складну структуру, тоді як середнього рівня було лише 15,4%. Усі решта являли собою найпростіші нейтральні веб-програми. «Погані» боти використовуються для організації кібератак, викрадення даних, таємного стеження за сайтами та користувачами, дезінформації та інших зловмисних цілей тощо. Цифрові боти стають усе більш поширеними та працюють у різних сферах обслуговування, оптимізації пошукових систем і розваг. Проте не всі боти мають «добрі» наміри – чимало з них можуть бути шкідливими.

Зловмисники та хакери продають журнали, зібрані шкідливими ботами на різних ринках, навіть у мережі «Darknet», створюючи потужні загрози. Таким чином, у світових масштабах набирають обертів продажі журналів шкідливих ботів. Саме бот використовує шкідливе програмне забезпечення з метою викрадення інформації. Це можуть бути реквізити кредитної карти або облікові дані в онлайн-банку. Боти можуть отримати доступ до особистого листування, фотографій, історій переглядів у браузері. Також з використанням ботів зловисники можуть видалити або заблокувати акаунти жертви (наприклад, Netflix, Spotify або Steam). Найпопулярніші типи шкідливого програмного забезпечення, які використовуються ботами для крадіжки та збору даних: «RedLine», «Vidar», «Racoon», «Taurus» і «AZORult». При цьому, сам «RedLine» є найпоширенішим. Наприклад, на платформі «Russian Market» ця програма займає понад 60% усього ринку, що переконливо засвідчує вірогідну можливість використання російськими хакерами та зловмисниками шкідливого програмного забезпечення за допомогою ботів для досягнення своїх цілей у кібервійні. Наприклад, шкідливе програмне забезпечення «Racoon», розроблене у 2019 році, отримує конфіденційні дані з широкого спектру додатків, включаючи 29 окремих браузерів та базі «Chromium», додатків на базі Mozilla. Після того, як «Racoon» отримує усі дані з інфікованого комп`ютера, відразу видаляє сліди своєї злочинної діяльності. Тобто використовуючи сучасні передові технології, зокрема шкідливі боти, держава-агресор активно вдається до їхнього використання у своїх злочинних інтересах.

Кремль прагне успішно маніпулювати свідомістю українців в соціальних мережах і пошукових системах, поширюючи брехню про збройні сили України та нагнітання істерії через соціально-економічні проблеми завдяки постам та коментарям у соціальних мережах від сотен тисяч ботів. На жаль, така

тенденція зберігається й по теперішній час. Також рф технологічно намагається використовувати боти щодо української та європейської аудиторії з метою поширення своїх наративів та масштабного збору інформації. Російські боти в соцмережах видають себе за справжніх українців та активно просувають наративи московії. Основні зусилля у поширенні російських ботів покладаються на головний науково-дослідний обчислювальний центр рф (ГОЛОВНІВЦ) – установу, яка виконує завдання фсб та підпорядковується безпосередньо адміністрації президента рф. Ця структура активно проводить кампанії з дезінформації та викрадення даних. Останнім часом рф демонструє тренд застосовувати боти з метою викрадення конфіденційної (таємної) інформації, оскільки лише 1% російських ботів вдається виявити та знищити [11]. У зв'язку з цим російський уряд став більш успішним у маніпулюванні рейтингами в соціальних мережах та пошукових системах навколо світу, поширюючи брехню за допомогою сотень тисяч фейкових акаунтів та ботів. «Google», «Meta» та інші гіганти технологічної індустрії намагаються зупинити ці процеси, проте рф прагне будь-яким чином обійти такі обмеження.

Так, 7 квітня 2023 року видання «The New York Times» повідомило про те, що в мережі були опубліковані секретні військові документи США, в яких йшлося про плани НАТО та Вашингтона збільшити допомогу Збройним Силам України перед контрнаступом, що мало російський слід та стало наслідком успішної дезінформаційної кампанії з боку кремля. Першочергово відповідні документи з'явилися в соціальних мережах «Twitter» і «Telegram» [12].

Російські спецслужби автоматично збирають інформацію з коментарів у телеграм-каналах або відкритих чатах. Для цього використовуються спеціальні «скринери», які відстежують активність користувача або чату в цілому. З метою анонімізації своєї злочинної діяльності особи, причетні до керування ботів, використовують різноманітні засоби, зокрема, недостовірні акаунти, віртуальні мобільні телефони, іноземні SIM-карти, віртуальні виділені сервери тощо. Російськими спецслужбами в інтересах країни-агресора нарощуються зусилля із використання такого інструменту інформаційної війни як створення на платформах соціальних мереж «Facebook», «Instagram» і «Twitter» мереж облікових записів (акаунтів) (так званих бот-мереж), які містять недостовірні дані щодо користувачів, діяльність яких є координованою ззовні та об'єднана єдиною метою, зокрема такою як проведення акцій інформаційного деструктивного впливу. Така діяльність з використання бот-мереж певним чином порушує політику конфіденційності та умови використання вказаних сервісів.

Зокрема, відповідно до політики співтовариства мережі «Facebook» у цій соціальній мережі заборонено створювати профілі і сторінки, власники яких видають себе за інших людей або порушують умови використання «Facebook». У разі порушення користувачем правил платформи йому заборонено створювати інші облікові записи (акаунти) без дозволу «Facebook». Крім того, мережа «Facebook» приділяє особливу увагу цілісності облікового запису і достовірності ідентифікаційних даних. Зокрема, грубим порушення правил спільноти є координація діяльності у рамках мережі облікових записів або інших об'єктів. Так, наприклад, тільки у січні-березні 2022 року «Facebook» видалив 1,6 млрд. фейкових акаунтів [13]. У квітні 2022 року соціальна мережа «Facebook» заблокувала створену в рф мережу акаунтів, спрямовану проти України та українських військових, які поширювали неправдиву та тенденційну інформацію на шкоду державним інтересам [14].

Правилами встановлені соціальною мережею «Instagram» не заборонено одному користувачу створювати декілька облікових записів (акаунтів), разом із тим політика конфіденційності платформи спрямована на протидію використанню підроблених облікових записів, при реєстрації яких використовуються ідентифікуючі дані інших осіб. Відповідно до правил «Twitter», користувачам заборонено використовувати недостовірні дані про особу, а саме фотографії профілю користувача, біографічні дані, інформацію щодо місцезнаходження профілю тощо. Саме величезна кількість російських ботів змусила власника «Twitter» Ілона Маска спочатку ввести плату за верифікований обліковий запис, а потім і зменшити можливість перегляду твітів для незареєстрованих користувачів.

Однозначно викликає певне занепокоєння використання найнебезпечнішого ресурсу для спілкування української аудиторії – російської соціальної мережі «Telegram», особливо в умовах війни. Російській месенджер «Telegram» у липні 2015 року відкрив платформу для створення ботів, які відкликаються на команди користувачів та взаємодіють із зовнішніми сервісами. Боти на базі платформи месенджера «Telegram» особливо популярні, завдяки її широкої аудиторії та високого ступеню захисту даних. Як ні парадоксально, для української аудиторії користувачів соціальних мереж та Інтернету саме телеграм-канали є першочерговим джерелом отримання інформації [15]. Ворожі боти у мережі «Telegram» можуть здійснювати фейкові коментарі або дописи у вигідному для держави-агресора руслі. Загальновідомо, що анонімні телеграм-канали мають величезну кількість проросійських активностей, а «Telegram» створив у собі спільноту, яка закрита від суспільства, при цьому цей месенджер наполонили боти, які викрадають акаунти користувачів.

Вітчизняні спеціалісти з безпеки нещодавно виявили нову шахрайську схему з клонування акаунтів у мережі «Telegram» [16]. Зловмисники підробляють імена каналів та груп, змінюючи букви у назві на ідентичні латинські символи. Такий спосіб створення фейкових каналів є досить простим, адже все, що необхідно зробити шахраям – створити новий канал або групу та замінити букви у назві. Зазвичай у фейкових групах розміщують фішингові посилання, при переході за якими користувачі можуть заразити свій ПК або смартфон шкідливим програмним забезпеченням. Також «працює» шахрайська схема з викрадення акаунтів у «Telegram» – зловмисники надсилають користувачам листи з проханнями взяти участь в онлайн-голосуванні, перейшовши за посиланням. Жертви нерідко вірять у такі повідомлення, адже їх надсилають облікові записи, які є в телефонних книгах користувачів, інформацію з них теж викрадають.

Оскільки російські спецслужби зазвичай використовують такі ж методи заволодіння інформацією, як звичайні кібершахраї або хакери, то саме фішинг під виглядом різних телеграм-ботів активно використовується нею задля досягнення своїх злочинних цілей. При цьому фішинг став одним із основних способів шахрайства у популярному месенджери, а зростання інтересу зловмисників та хакерів до платформи «Telegram» обумовлений притоком аудиторії, які перейшли до цього месенджера з інших сервісів. Тільки у 2022 році фішинг

у мережі «Telegram» продемонстрував зростання на 800%, при цьому робочим інструментом зловмисників стали саме боти. У цьому месенджері чимало шахрайських угрупувань, які власне координують дії ботів. Використовуються схеми, які передбачають викрадення інформації за допомогою фейкових ресурсів, на яких тим чи іншим способом користувачів стимулюють ввести персональні дані, які необхідні для входу до месенджера. Основною метою є злом акаунтів користувачів з подальшим перехопленням контролю над популярними групами або каналами. На думку експертів, ще більш загрозу, аніж фішинг представляє новий метод авторизації в месенджері, який з`явився після того, коли «Telegram» перестав відправляти код авторизації за допомогою SMS, замінивши цей механізм на використання двофакторної аутентифікації (two-factor authentication, 2FA) через систему «активний клієнт» на мобільному пристрої або ПК.

Таким чином, месенджер «Telegram» залишається каменем спотикання, особливо враховуючи такі фактори, як: – він не підпадає під дію закону України «Про медіа», хоча більшість українських ЗМІ мають власні канали; – відсутність зворотного зв'язку з компанією-розробником; – наявна активність росіян у соціальній мережі; – існування анонімних каналів з невідомими авторами; – відсутність способів здійснювати контроль над сплатою податків телеграм-каналами тощо. На цьому фоні цілком логічно обмежити використання або навіть заборонити «Telegram» на період воєнного стану, оскільки через боти у цьому сервісі російські спецслужби масово закидують фейкові новини та пропагандистські матеріали деструктивного контенту, які розраховані на українську аудиторію користувачів.

На жаль, соціальні мережі не досить активно реагують на повідомлення про фейкові профілі і сторінки, які причетні до проведення інформаційних атак. Певним чином вирішення цього питання, особливо в умовах інформаційної війни рф проти України, можливо завдяки використання фактчекінгу – комплексного процесу, який являє собою перевірку фактів у відкритих джерелах інформації та містить пошук першоджерел інформації, дат створення фото та відео, перевірку біографії певного експерта тощо. Важливим напрямком виступає й кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації та які включають: – перевірку безпеки активних акаунтів; – аналіз програм; регулярне оновлення програмного забезпечення; – встановленя надійного пароля; – постійне резерве копіювання тощо. Правила кібергігієни допоможуть своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації, у тому числі й шпигунській діяльності російських ботів у соціальних мережах.

Актуальним інструментом і є клоакінг (від англ. cloaking – маскування) – сучасний сервіс фільтрації трафіку, який передбачає, у тому числі, введення в оману пошукових ботів, модераторів соціальних мереж. Під час клоакінгу створюється декілька різних за змістом веб-сторінок для звичайних користувачів, модераторів, пошукових ботів. В основі клоакінга перебувають спеціальні скрипти, які виконуються у веб-сервері. Коли до сервера спрямовується запит, він визначає хто саме звернувся: модератор чи звичайний користувач. Клоакінг надає змогу захистити контент від зовнішнього копіювання, шпигунських сервісів та забезпечити надійний захист систем від шкідливих ботів.

Розробка методу виявлення окремих ботів або бот-мереж потребує здійснення аналізу їх архітектури та можливостей, оскільки на сьогодні не існує загальноприйнятого чіткого стандарту стосовно їх структури, класифікації, можливих зловмисних дій. Тому при розробці методів їх виявлення необхідним є здійснення представлення об'єкта дослідження формалізованими загальноприйнятими засобами та його функційних можливостей. Керування бот-мережею здійснюється зловмисником через командно-контролюючий центр безпосередньо або через інші проміжні віддалені контролюючі центри [17, с. 185].

Окрім того, цю проблему, варто вирішувати законодавчими змінами. Зважаючи на чисельні зростання негативних наслідків для нашої держави, зокрема у ході війни рф проти України, які завдаються шляхом створення з метою збуту і використання облікових записів, що містять завідомо неправдиві відомості щодо користувача, задля організації здійснення інформаційних атак з поширенням тенденційної та недостовірної інформації, що загрожує національним інтересам України, вбачається актуальним і логічним запровадження кримінальної відповідальності за вчинення таких дій.

Слушно в цьому контексті вказує професор Д. Олєйніков, що на жаль, у чинному законодавстві не передбачено порядку створення облікових записів на соціально орієнтованих платформах та інших ресурсах, не закріплено обов'язку користувачів при цьому вказувати свої анкетні дані, за якими вони можуть бути ідентифіковані [18, с.177]. Доцільно вказати, що у серпні 2023 року в ЄС набув чинності закон про цифрові послуги (Digital Service Act, DSA) [19], який має на меті посилення боротьби з дезінформацією та нелегальним контентом в мережі Інтернет. Відповідно до цього закону великі технологічні платформи та пошукові системи з аудиторією понад 45 млн. користувачів на місяць повинні суворо стежити за контентом, що розміщується, і сплачувати збори наглядовим органам. Станом на 1 листопада 2023 року дія цього закону поширюється на 19 платформ та пошукових систем, зокрема AliExpress, Amazon Store, AppStore, Bing, Booking, Facebook (належить корпорації Meta), Instagram, Google Maps, Google Play, Google Search, Google Shopping, LinkedIn, Pinterest, Snapchat, TikTok, X (раніше Twitter), Wikipedia, YouTube та Zalando. Зазделегідь готуючись до набуття чинності законом, платформи запровадили нові способи для європейських користувачів позначати незаконний онлайн-контент і оманливі продукти, які компанії будуть зобов'язані швидко та оперативно видаляти, включаючи боти.

Висновки. З появою нових досягнень в сфері інтернет-технологій кремль через шкідливі боти намагається використовувати їх у своїх амбітних геополітичних інтересах. Адже використання ботів постійно набирає обертів. Актуальним є питання ефективної протидії інформаційним атакам з використанням ботів на замовлення російських спецслужб. Інформаційна війна рф в українському інформаційному просторі ведеться, серед іншого, із залученням цілої армії ботів у соцмережах. Мета їхніх дописів – сіяти зневіру, паніку, брехню серед українців, викрадення персональних та конфіденційних даних. Завданням російських інформаційних кампаній з використанням ботів є: деморалізація українців; акцентування уваги на розбіжностях

серед західних союзників та партнерів; збільшення можливостей рф у сфері контролю свого внутрішнього інформаційного середовища та просування проросійських наративів за кордоном. На підставі узагальнення результатів проведеного дослідження цілком логічно визначити організаційно-технічні аспекти протидії російським ботам, зокрема це: – обмеження використання або навіть заборона месенджеру «Telegram» на період воєнного стану; – системне використання фактчекінгу та заходів кібергігієни; – застосування сучасного сервісу фільтрації трафіку – клоакінга; – використання методів виявлення окремих ботів або бот-мереж на підставі аналізу їх архітектури та можливостей.

Окрім того, вважаємо доцільним прискорити схвалення законопроекту № 9223 від 19.04.2023 року [20], положення якого спрямовані на посилення кримінальної відповідальності за створення, придбання, використання або збут облікових записів, що містять завідомо неправдиві відомості щодо користувача, в інформаційних (автоматизованих), електронних комунікаційних мережах за допомогою яких поширюється недостовірна інформація (у тому числі від імені інших осіб, причетність яких до оприлюднення інформації не підтверджена). Це надасть змогу посилити кримінально-правовий захист інтересів держави в інформаційній сфері, сприятиме підвищенню ефективності боротьби проти інформаційних атак та інформаційних кампаній російського походження, які підвищують рівень соцальної напруги в суспільстві.

Література:

1. Гуржій С.В. Сучасні загрозливі тенденції використання telegram-каналів на шкоду державним інтересам. *Інформація і право.* 2021. № 4 (39). С. 162-169.
2. Voitovych, O., Kupershtein, L., & Holovenko, V. (2022). Виявлення фейкових облікових записів в соціальних мережах. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2(18), С.86–98. https://doi.org/10.28925/2663-4023.2022.18.8698
3. Кантур О.М. Актуальні проблеми протидії інформаційним загрозам у соціальних медіа під час повномасштабного вторгнення Росії в Україну. *Наукові записки Інституту законодавства Верховної Ради України.* 2022. № 2. С. 102-110. – URL: https://doi.org/10.32886/instzak.2022.02.11.
4. Котихова Л. Дослідження використання ІТ для протидії поширенню російської дезінформації в медіапросторі в умовах війни. *Вісник Приазовського Державного Технічного Університету. Серія: Технічні науки*. 2022. (44), С. 5-9. https://doi.org/10.32782/2225-6733.44.2022.1
5. Левін О. Використання фейкових акаунтів як інструмент ІПСО під час українсько-російської війни. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2023. № 2 (123). С. 89-94.
6. Панченко О.А. Інституційне забезпечення процесів протидії російській інформаційній експансії та пропаганді в сучасному світі. *Інформація і право.* 2021. №3 (38). С. 28-34. URL: https://ippi.org.ua/sites/default/files/5_22.pdf
7. Поляков О.М. Особливості протидії поширенню деструктивного контенту. *Інформація і право.* 2023. №1(44). С. 129-141.
8. Лисько Т.Д., Паламарчук В.О. Ботоферми та інші кіберзагрози під час воєнного стану: питання кримінальної відповідальності. *Юридичний науковий електронний журнал.* 2022. №11. С. 570-572. https://doi.org/10.32782/2524-0374/2022-11/138
9. Юшков А.Г. Загрозливі тенденції використання ботоферм на шкоду державним інтересам України: механізми запобігання та протидії. *Інформація і право.* 2021. №3(38). С. 90-98.
10. Боти генерують майже половину інтернет-трафіку світу URL: https://24tv.ua/tech/mayzhe-polovina-svitovogo-internet-trafiku-nalezhit-botam_n2321537
11. Russians boasted that just 1% of fake social profiles are caught, leak shows URL: https://www.washingtonpost.com/technology/2023/04/16/russia-disinformation-discord-leaked-documents/
12. Ukraine War Plans Leak Prompts Pentagon Investigation URL: https://www.nytimes.com/2023/04/06/us/politics/ukraine-war-plan-russia.html
13. Фейкові друзі. Чому соцмережі заполонили шахраї і як з ними боротися URL: https://www.epravda.com.ua/publications/2022/08/13/690089
14. Закликали здатися українських військових. Facebook заблокував російську та білоруську мережу акаунтів URL: https://ms.detector.media/sotsmerezhi/post/29329/2022-04-12-zaklykaly-zdatysya-ukrainskykh-viyskovykh-facebook-zablokuvav-rosiysku-ta-bilorusku-merezhu-akauntiv/
15. Загальні суспільно-політичні настрої та джерела інформації URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1307&page=1
16. Росіяни створюють клони українських медіа URL: https://glavcom.ua/country/incidents/rosijani-stvorjujut-kloni-ukrajinskikh-media-958263.html
17. Савенко О.С. Виявлення бот-мереж розподіленими системами на основі класифікації. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки.* Том 30 (69). 2019. №2. Ч.1 С. 183-191.
18. Олейніков Д.О. Критичний аналіз проекту закону України №9223 від 19.04.2023 в частині кримінальної відповідальності за дії, передбачені ст. 114-3 КК України. *Науковий вісник Ужгородського національного університету.* 2023. Серія «Право». Випуск 77. Частина 2. С. 175-180.
19. Digital Service Act (DSA) URL: https://www.eu-digital-services-act.com
20. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо встановлення відповідальності за окремі дії проти основ національної безпеки України: проект закону №9223 від 19.04.2023 року URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1738124

Hurzhii S. Organizational-technical and criminal-legal fundamentals of countering russian bots in the conditions of war

Summary. The article is devoted to the reasech of the problem of the spread of russian bots in social networks and the development of effective means of preventing such manifestations. The trends in the spread of fake accounts and bots in the russian Federation for the purpose of manipulating consciousness, spreading anti-Ukrainian narratives, stealing personal data and confidential information have been determined. The threats of the use of russian bots in socially oriented Internet resources for the purpose of carrying out destructive and subversive information activities to the detriment of the national interests of Ukraine are outlined. The concept, content and features of bot activity in social networks are revealed. It is emphasized that in the modern world, bots generate almost half of the world's Internet traffic. The role and place of bots during their use by attackers for the purpose of spreading malicious software is defined. The mechanisms of using bots during the information war of the russian federation against Ukraine are considered, and the goals and objectives of russian global information campaigns of influence are determined. The methods of work of the russian special services in increasing efforts to use such a tool of information warfare as the creation of accounts (accounts) containing unreliable data about users

on the platforms of social networks "Facebook", "Instagram" and "Twitter" in order to carry out information destructive actions are detailed. The principles of the privacy policy of such services as "Facebook", "Instagram" and "Twitter" regarding the use of fake accounts during registration as identification data of other persons have been determined. The risks of using the "Telegram" social network in Ukraine were considered. Prerequisites, risks and threats of phishing when using the Telegram social network are defined. The role of fact-checking and cyber hygiene as important components of the prevention of detection, blocking and destruction of Russian bots is fixed. The relevance of the application of the cloaking procedure in order to strengthen the protection of content against external copying, spy services and malicious bots is substantiated. The directions of the improving the current legislation with the aim of limiting the use of the Telegram network in Ukraine are summarized. The directions for the development of effective mechanisms for countering information attacks with the use of bots, which threaten the national security of Ukraine, were determined by the special services of the russian federation. The European experience of legislative provision of combating disinformation and illegal content in social networks and well-known Internet services is revealed. On the basis of the generalization of the conducted research, the organizational and technical foundations and criminal and legal principles of preventing the destructive activity of russian bots in social networks and in the worldwide global network have been determined.

Key words: account, bot, national interest, war, fake, content, social networks, fact-checking, cyber hygiene, cloaking, phishing.