# 10.5. Боти, тролі та їх діяльність

## Ботнет

Силу кібератак в Інтернеті можна порівняти з вибухом атомної бомби в реальності. Сьогодні недооцінювати серйозність хакерських зломів веб-ресурсів нерозумно і небезпечно. З такою напастю борються фахівці, на яких влада витрачає мільйони і мільярди доларів.

Ботнет (botnet) є мережею комп'ютерів, заражених шкідливим кодом, який дозволяє злочинним угрупованням дистанційно керувати «інфікованими» машинами без відома користувача.

Бот - це шкідлива програма, яка втілюється на комп’ютер і надає функції віддаленого керування кіберзлочинцям, а сам заражений комп'ютер перетворюється на «зомбі». Комп'ютер, який керує ботнетом, називається центром управління. Правда, щоб не розміщувати в одному місці управління великим ботнетом, зловмисники розділяють його на кілька дрібніших, на випадок, якщо один з них вийде з з ладу. Ботнети можуть складатися від кількох сотень комп'ютерів до десятків або сотень тисяч комп'ютерів-зомбі.

В певний момент за командою організатора атаки «зазомбовані» комп'ютери одночасно зв'язуються з сайтом, якому належить стати жертвою, і надсилають до нього певний запит. Ця дія сама по собі не може завдати шкоди сайту. Але через неочікувану величезну кількість запитів, якої не буває в нормі, комп'ютерна система припиняє роботу.

Розробники ботів намагаються зробити так, щоб ці шкідливі програми довгий час не видавали своєї присутності на комп’ютері. Тому, багато власників інфікованих комп'ютерів не підозрюють про зараження. Серед підозрілих ознак може бути хіба що уповільнення роботи системи, поява дивних повідомлень, іноді може трапитися збій. В той же час, у разі виявлення Інтернет-провайдером фактів поширення з інфікованого комп’ютера шкідливого програмного забезпечення, спаму або масового DDoS-трафіку, провайдер може відімкнути цей комп’ютер від Інтернету.

Боти проникають на чужі комп'ютери в різний спосіб. Найчастіше вони поширюються через сумнівні сайти, при завантаженні неперевірених плагинів для браузера, через електронні повідомлення, із запуском генераторів ключів, «кряків», патчів та іншого піратського програмного забезпечення. Є також варіант зараження від флешки, якщо вона побувала на зараженій машині.

Вилучити заражений комп'ютер з ботнету дуже просто - достатньо відімкнути його від Інтернету. Однак в епоху повсюдного Інтернету такий спосіб видається вкрай небажаним: це ускладнить доступ до інформації, й немає гарантії, що вірус не підхопиться від флешки.

#### Основні ознаки зараження комп'ютера і належності до машин ботнету.

* Програмне забезпечення посилено звертається до Інтернету, намагаючись встановити зв'язок з провайдером в будь-який час, коли комп'ютер включений.
* На порядок збільшується мережний трафік.
* В системних процесах з'являється багато нових, яких раніше не було, причому нові процеси маскуються під системні (тобто мають схожі з ними імена).

Ботнети виробляють атаки на сервери, здійснюють збір і передачу секретної інформації, розсилають спам, здійснюють фішинг і накрутку лічильників, при кліці на які виплачуються нехай і копійки, але якщо в ботнет сотні комп'ютерів, то це вже не копійки, а цілком реальні гроші. Треба зауважити, що всі перелічені дії ботнет може здійснювати одночасно.

### Поширені загрози від мережі ботнетів

**DDoS-атаки.** Метою є переповнення буфера атакованої машині, в результаті чого вона перестає відповідати на будь-які запити і просто «висне». DDoS-атаки широко використовуються хакерами для отримання доступу до атакованих комп'ютерів і запуску на них коду. Часто застосовуються недобросовісними конкурентами, оскільки DDoS-атака не є дорогим заходом, а усунення її наслідків може потребувати багато грошей і часу.

**Збирання секретної інформації.** Секретна інформація різного роду, що не призначена до широкого розголошення, завжди привертала кіберзлочинців. Бот на комп’ютері - це шпигун, який може надсилати з інфікованого комп'ютера паролі до різних сервісів, робити знімки екрану, виконувати пошук файлів з подальшим їх видаленням або завантаженням на віддалений сервер. Це номери кредиток, і паролі до електронних гаманців, логіни, паролі та списки контактів до поштових скриньок чи Скайпу і багато іншого. Отримана інформація при цьому використовується як самими зловмисниками, так і продається на сторону.

**Спам-розсилки.** Якщо зловмисник отримає список контактів з поштової програми користувача, то його база для спам-розсилки збагатиться на кілька десятків, ну, може сотню e-mail-адрес, але в ботнет кілька тисяч комп'ютерів і це вже суттєво. Є ймовірність що комп'ютер користувача можуть занести до чорного списку як злісного поширювача спаму.

**Пошуковий спам.** Застосовується для підвищення рейтингу деяких сайтів в пошукових запитах. Чим більше відвідувачів на сайті, тим більше його власник отримає прибутку від реклами.

**Збільшення клік-лічильників.** Існують як окремі сайти, так і цілі мережі, які готові платити за перехід по їх посиланнях в надії, що користувач, який перейшов за посиланням здійснить в них покупку. Цим і користуються власники ботнетів, змушуючи комп'ютери жертв переходити за потрібними посиланнями і заробляючи при цьому непогані гроші.

**Фішінг.** Фішингом називають створення підробленої сторінки популярного проекту. Користувач прямує туди, і його просять авторизуватися і гроші з гаманців користувачів переходять до злочинців.

### Організація мережі ботнетів

Нажаль, організувати ботнет зовсім нескладно, в Інтернеті багато інструкцій щодо його створення. Але, насамперед, зловмисникам потрібно тим або іншим чином втілити бот на комп'ютер жертви, тому, слід бути уважними і не запускати застосувань, які надіслано невідомими особами.

Використання ботнетів далеко не завжди здійснюється власником мережі: за придбання або оренду мережі ботнетів може заплатити якась рекламна компанія. Цілеспрямоване створення ботнетів на продаж є цілком прибутковим кримінальним бізнесом.

### Рекомендації щодо захисту від ботнету

* Встановити на комп'ютер хороший антивірус і регулярно оновлювати антивірусні бази.
* Встановити і регулярно оновлювати брандмауер.
* Встановлювати всі оновлення до операційної системи та програмного забезпечення, що випускається розробниками цих продуктів.
* Використовувати шифрування для конфіденційних даних.
* Бути пильними і обережними при завантаженні файлів, особливо з незнайомих або варезних серверів.

# Боти в соціальних мережах

Численні спроби розібратися в причинах несподіваної перемоги Дональда Трампа на президентських виборах в США в 2016 році показали світу, як політики і їх команди використовують соціальні медіа для досягнення своїх цілей. Концентрація ботів на сторінках окремих політиків може досягати 50%, але в більшості - це низькоякісні акаунти, що зроблені не профільними IT-компаніями, а кустарними фермами.

## Боти і їх ферми

Типова історія розвитку Facebook-сторінки або акаунта українського політика складається з трьох послідовних кроків. Перш за все, для поліпшення свого мережного іміджу, його PR-команда створює 5-10 фейкових акаунтів, які потрібні, щоб пом'якшувати гострі теми і просувати потрібну думку в аудиторію.

Однак, таку стратегію складно масштабувати, результат часто не такий, як очікувалося, і незабаром незадоволений політик переходить до наступного кроку - наймає команду SMM-фахівців. Вони повинні писати за нього багато «гарних» і «правильних» постів, заряджених на потік лайків. І третій крок – співпраця з компаніями, що спеціалізуються на ботофермах. Ботоферми можна вважати базовим інструментом впливу на думку українських користувачів соцмереж.

### Найбільш поширені різновиди ботів:

**Боти-одноденки**. Незграбно створені акаунти без фото профілю, невеликою кількістю друзів, з порожньою або забитою репостами стрічкою (рис.1). Створюються, як правило, автоматично за допомогою скриптів, які можна знайти в мережі. Такі боти щодня здійснюють величезну кількість однотипних дій, завдяки чому Facebook досить швидко їх викриває і блокує. Оскільки завданням цих ботів є доведення меседжу і зникнути після бану, то автори не особливо намагаються робити їх схожими на реальних людей. Залежно від активності їх життєвий цикл становить від однієї доби до кількох місяців.

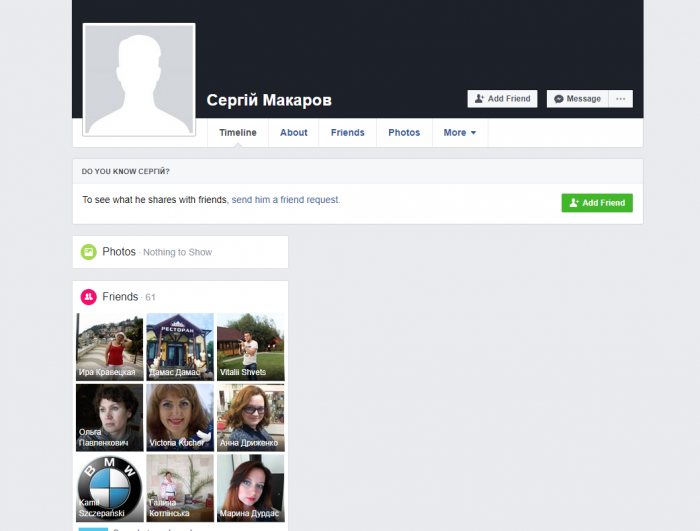


Рис.1. Приклад соціальної сторінки бота-одноденки

**Класичні боти** - відрізняються від одноденок наявністю картинки-кавера і фото профілю - з квітами, кошенятами, агітаційними картинками і практично ніколи - з людиною (рис.2). Такі акаунти створюються більш просунутими версіями скриптів, рідше - вручну. Більш якісне заповнення сторінки дозволяє таким акаунтам прожити трохи довше, ніж одноденкам.



Рис.2. Приклад соціальної сторінки класичного бота

**Боти-іноземці** - акаунти з екзотичними іноземними іменами, що куплені задешево на закордонних ботофермах. Ціна коливається в залежності від країни-виробника. В цілому, це досить поширений бізнес в ряді країн третього світу, де акаунти виробляються в промислових масштабах і коштують дешево. Тільки, наприклад, в Лаосі кількість зареєстрованих користувачів Facebook в 1,3 рази перевищує загальну кількість користувачів Інтернету серед населення країни. В іншому, зовнішні ознаки ботів-іноземців цілком відповідають класичним роботам (рис.3.).

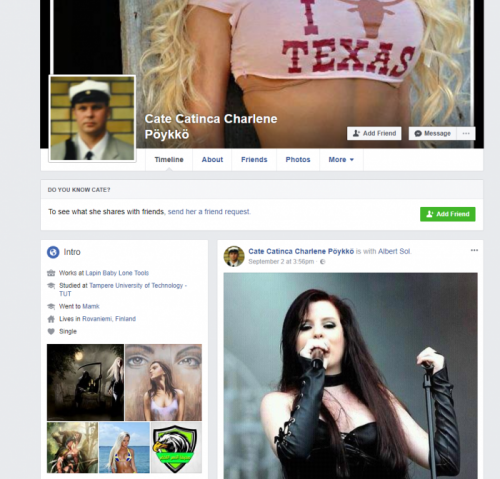


Рис.3. Приклад соціальної сторінки бота-іноземця

Практичної користі від таких акаунтів мало. За ними не стоїть сегментована аудиторія, вони не збільшують охоплення постів. Проте, вони ідеально служать для того, щоб у сторінки замовника за ніч з'явилося сто тисяч передплатників, як це кілька років тому сталося з акаунтом Віктора Медведчука.

Як правило, замовники не усвідомлюють, що від низькоякісних ботів шкоди більше, ніж користі. Алгоритми Facebook легко обчислюють такі облікові записи, після чого або зменшують позицію сторінки у видачі або навіть блокують. Описані вище категорії професіоналами використовуються хіба що для того, щоб підставляти опонентів. Але, незважаючи на це, саме такий інструментарій найбільш поширений на ринку і більшість всіх штучних дій на політичних Facebook-сторінках здійснюється саме за його допомогою.

## Віртуальні особистості та інші маріонетки

По сусідству з ботами розташувалися штучно створені акаунти, розвитком і доглядом яких займаються реальні люди. Залежно від призначення, часу і зусиль, витрачених на догляд акаунту, сторінки віртуальних особистостей можуть бути як схожими на роботів, так і не відрізнятись від живих людей. Їх можна розділити на кілька типів:

**Акаунти з бірж лайків.** Якщо у вас немає лайків, але дуже хочеться - їх можна купити на профільних біржах, де за гроші пост отримає тисячі лайків. Купити там можна практично будь-які дії - лайки, поширення, коментарі, підписки на сторінки. Незважаючи на те, що майже всі біржі гарантують, що в них працюють реальні люди, насправді багато акаунтів є агрегаторами міні-ботоферм. Відповідно, при просуванні акаунту через таку біржу замовник отримує зменшення рейтингу і блокування.

На деяких біржах дійсно є реальні користувачі, але робота з ними не гарантує якості взаємодії і тривалого ефекту. Широко поширена практика, коли користувач замовляє лайки, отримує їх, оплачує роботу, а через певний час акаунти відкликають свої лайки назад і замовник це втрачає, але з марно витраченим бюджетом.

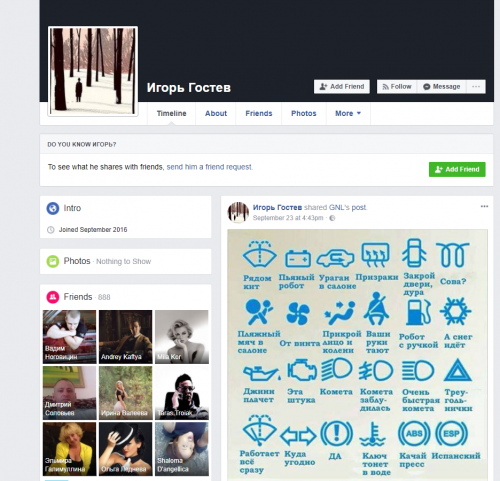


Рис.4. Приклад соціальної сторінки біржі лайків

Приклад біржового акаунту: є аватар, але немає фото профілю, каверу, особистих фото, стрічка складається з репоста, незважаючи на 888 друзів, взаємодії з постами немає (рис. 4).

**Акаунти з шаблонним просуванням** - за їх розвиток відповідає скрипт або реальна людина. Як правило, якість таких акаунтів є вищою: є аватар, відкриті друзі, оновлюється стрічка. Але, якщо придивитися, то пости в стрічці з'являються приблизно в один і той же час з одних і тих же джерел. Під постами немає взаємодій або зустрічаються самотні коментарі та лайки. Акаунти з шаблонним просуванням - це наступна за поширеністю категорія ботів, до послуг яких вдаються в українському Facebook.

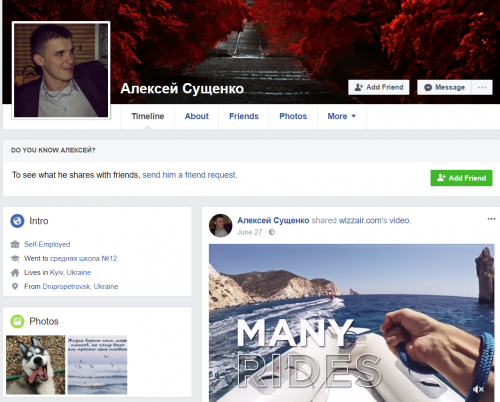


Рис.5. Приклад соціальної сторінки з шаблонним просуванням

Фото профілю і обкладинка є, але особистих фото немає. Фотографія профілю явно знайдена в пошуковій системі (рис.5). При 80+ друзях з лайками у постів небагато.

**Акаунт з нешаблонним просуванням** - бот з поведінкою, яка схожа на дії живої людини. У таких акаунтів в стрічці використовуються різні типи постів, під якими зустрічаються самотні лайки або коментарі (рис.6). Плюс - ці сторінки дійсно нагадують сторінки реальних людей. Мінус - через розпорошеність постів в акаунта може не бути чітко сегментованої аудиторії.



Рис.6. Приклад соціальної сторінки з нешаблонним просуванням

**«Жива людина»** - акаунти, що створюються складною програмою, яка переконливо імітує дії людини в соціальній мережі. Завдяки цьому вони не викликають підозр у Facebook, оскільки є невидимими для його алгоритмів обчислення спамерських пошукових роботів. «Живі люди» акумулюють в друзях і передплатниках активну аудиторію і регулярно взаємодіють з нею.

Розпізнати віртуальність такого акаунту зможе не кожен фахівець - для цього потрібно задатися такою метою, знати де шукати вади і витратити чимало часу. За великим рахунком, далеко не кожна сторінка реального користувача мережі виглядає так правдоподібно, як ці акаунти. Тому, користувачі навіть не здогадуються, що бачать в стрічці контент, створений машиною.

Боти-«живі люди» ретельно збирають і бережуть свою аудиторію. Це цікава і цінна категорія, оскільки з її допомогою замовник дійсно може досягти реальних результатів. Такі боти здатні формувати або змінювати інформацію в соціальній мережі, впливати на думку простих людей, журналістів, політиків.

**Боти-ЛГД.** Бездушні Лідери Громадської Думки. Вершина серед спамерських пошукових роботів. Створені вручну і старанно підтримувані акаунти. Кожен з них має своє позиціонування і свою аудиторію. В багатьох з них дійсно цікавий і унікальний контент. Таких акаунтів мало і вони використовуються для вкидань необхідної замовнику інформації, а не для її масштабування - для розгону їм на допомогу залучаються боти простіше і дешевше.

## Люди та інші публічні майданчики

Звинувачуючи в інформаційному спамі ботів, не слід забувати про реальних людей, які не мають жодного відношення до ботів, але працюють в соцмережах в чиїхось інтересах.

**Лідери громадської думки.** Експерти, журналісти, публічні персоналії і просто люди, чиї акаунти знайшли масову популярність. За гроші, інші форми винагороди або просто за покликом серця пишуть про те, що цікаво замовнику. ЛГД різного рівня підготовки є у всіх політичних сил. Незважаючи на потужний ресурс популярності, ставлення до ЛГД в українському Інтернеті можна класифікувати як скептичне. З одного боку, в кожного лідера думок є аудиторія, вслухається до кожного слова, з іншого - критика ідеологічних супротивників і дискредитація за рахунок проплачених публікацій.

**Прості користувачі Facebook.** Змусити звичайних користувачів писати про те, що необхідно замовнику - вищий пілотаж. Досягається він двома способами - вихованням потрібної аудиторії або загортанням її в правильний інформаційний кокон.

Перший варіант - простий, але нестабільний, оскільки мова йде про регулярне залучення великої кількості людей, яке мотивується лише ідеями. У хід йдуть регулярні гасла, заклики, акценти на подразники, соціальні проблеми і т.д. Особливо складно утримувати контроль в період політичного міжсезоння, коли інформаційних приводів мало, а компромат на опонентів дотримується на час ближче до виборів.

Другий варіант є складнішим і вимагає більше часу на підготовку, проте, за рахунок того, що навколо цільової аудиторії створюється потрібне інформаційне поле - забезпечує більш тривалий ефект, коли реципієнти меседжу здійснюватимуть потрібні дії або поширювати інформацію на постійній основі, не здогадуючись про те, що ними хтось керує.

Також в формуванні інформаційного поля широко використовуються пабліки і групи, але їх роль поступово слабшає. Причини цього дві: алгоритм Facebook, який надає їм низький ранг при видачі поста в стрічку, а також низька якість контенту таких пабліків і груп, що помножені на шкідливі і несистемні інструменти їх просування.

Паблік - це скорочення від «публічна сторінка», яку також можна створити в соцмережі. Це сторінка, що подібна до сторінки користувача, але створюється для відображення і споживання інформації на якусь певну тему бренда, компанії, відомої особи. Група – це сторінка (закрита чи відкрита) для однодумців по різних інтересах.

Для формування потрібного інформаційного поля найчастіше використовуються такі майданчики:

1. **Паблік великих ЗМІ і ідеологічні паблік.** Тут сконцентрована стабільна і лояльна аудиторія. Це хороші і дорогі точки вкидання.
2. **Паблік ЗМІ другого рівня** - неоднорідна категорія. Серед них є добре розкручені майданчики, місячні рекламні бюджети яких вимірюються тисячами доларів. Але їх завдання не в формуванні інформполя в Facebook, а в тому, щоб генерувати трафік, перескеровувати його на майданчик сайту і там продавати.
3. **Паблік-інтегратори популярного контенту.** Незважаючи на непоганий заробіток на трафіку, такі майданчики складно використовувати для політичних або бізнес-вкидань, оскільки їх контент не підходить для таких цілей і не отримує підтримки у необхідної цільової аудиторії.
4. **Мертві пабліки** – які раніше були створені для вкидань, розгойдувалися на старті. Потім необхідність в них відпала, вони тривалий час були заморожені і активізуються час від часу під конкретне замовлення.
5. **Групи** - в силу обмеженого числа членів, є неефективними для поширення інформації. Можуть ефективно використовуватися для координації зусиль. Ряд політичних сил використовує закриті групи для поширення «темників» серед своїх прихильників і координації їх дій. Це все корисне, що з них можна вичавити для політичних цілей.

Типові завдання, які виконуються за допомогою таких майданчиків:

1. **Вкидання інформації через Facebook** - підсумковий результат залежить від якості аудиторії, на яку працює інструмент та її лояльності. При вкиданні важливо, хто першим на нього відреагує, оскільки це визначає швидкість подальшого поширення.
2. **Розгін інформації** - тут важливим є не кількість, а якість акаунтів. Наприклад, 300 акаунтів з грамотно сформованою аудиторією потенційно можуть акумулювати в друзях 100 000 активних в Facebook українців.
3. **Попадання в потрібні новинні стрічки** - тут потрібні акаунти, які акумулюють у себе окремий сегмент аудиторії соцмережі - наприклад, журналістів чи політиків.
4. **Тролінг опонентів** - важливо не тільки відшукати вразливість, але і розтиражувати її через правильно підібрані акаунти.
5. **Просування акаунту політика або паблік партії**

## Вартість ботнетів

Ціна на ботнет залежить від якості акаунтів і наявності автоматизованих процесів.

### Дешево і погано

Найпримітивніший інструментарій по роботі з Facebook-спільнотою. Вартість такої роботи починається від $100 за проект і вимірюється кількістю куплених лайків, комментарів і поширень. В основному, використовуються російські та азійські боти з категорії ботів-одноденок.

### Ручна робота з елементами автоматизації

Компромісний і тому найбільш поширений зараз формат. Поділяється на:

1. **Фрілансери** - продають лайки, коментарі і поширення. Використовують біржі як свій елемент автоматизації. Забезпечують низьку якість коментарів і акаунтів, але при цьому доступні за вартістю послуг. Середній чек - близько $ 300 за тиждень роботи.
2. **Класичні комерційні ботоферми** - постійний штат, що працює в кілька змін. Автоматизація мінімальна - як і фрілансери використовують біржі. Активно працюють з ЛГД. Забезпечують контрольовану якість роботи. Можуть забезпечити високі охоплення. Через ручну роботу над ботами, вартість послуг висока і обчислюється тисячами доларів за тижневий проект.
3. **Своя політична ботоферма** - типовий випадок для великих партій. Якість ботів середня або низька. Рівень автоматизації теж низький. В період виборів робота йде в цілодобовому форматі, в міжсезоння - в більш вільному форматі. Вартість послуг залежить від розміру партійного гаманця, поділеної на кількість фантазій відповідального функціонера.

### Максимальна автоматизація

Якісна і дорога. В продуктах такого типу автоматизація досягає 80%, а в основі - акаунти типу «живі люди», за якими стоїть реальна аудиторія. В основному, це великі ферми, які персоналізують свої ресурси під конкретного замовника. В арсеналі таких ферм тисячі акаунтів і автоматизація всіх проектних процесів, що дозволяє реалізовувати найскладніші інформаційні завдання за лічені години.

Незважаючи на те, що цей варіант потребує великих стартових витрат, при тривалій кампанії він буде найбільш оптимальним за вартістю. Бюджет тижневого проекту тут може починатися з кількох сотень доларів при високій якості результату.

## Боти, яких обирають користувачі

Незважаючи на велику кількість вибору, український політикум при роботі з аудиторією соціальних мереж поки що звертає увагу на базові і бюджетні рішення по роботі з аудиторією. Через сильно недовіру до нових технологій і через великі сподівання на пенсіонерів, яким достатньо білбордів та інших традиційних методів агітації.

Контент для ботів пишеться через біржі або фрілансерів, більша частина всіх процесів щодо просування ферм і реалізації проектів здійснюється вручну. Невеликі ферми часто використовують одні й ті ж акаунти в десятках проектів паралельно, що видно в стрічках самих акаунтів, або ж часто кардинально змінюють політичну орієнтацію.

Через слабку автоматизацію та спрощені алгоритми, які використовуються українськими політиками методи роботи з Facebook-аудиторією, м'яко кажучи, не відпрацьовують свої інвестиції. Коли по боту зрозуміло, що він не жива людина - яка від нього користь, окрім репутаційних втрат для замовника?

Рішення, що побудовані на автоматизації та машинному навчанні, ймовірно витіснять примітивні ботоферми. Питання в тому, хто з політичних гравців першим зверне на них увагу і використовує для того, щоб вирватися в електоральні лідери. Вірусний контент з потрібною ідеєю - це digital-гречка найближчих виборів, теплий інформаційний кокон, в який приємно загорнутися напередодні традиційного невдоволення опалювальним сезоном.

## Тролі і тролінг

Троль - це хуліган в Інтернеті, що провокує людей на словесну сварку в коментарях. Це означає, що користувач може зіткнутися з таким персонажем, любителем покритикувати на любій площадці, яка відкрита для коментарів і створено для спілкування чи обговорення: блог, форум, соціальні мережі.

Троль завжди свідомо стає її зачинателем. Розпалюючи конфлікт, він отримує задоволення від створеного ним спору, спостерігаючи, як люди між собою сваряться.

### Як розпізнати троля?

Особливість Інтернету в тому, що тут будь-яка людина може носити маску, сховавшись за аватаром і ніком. Відчуття безкарності і безпеки надають йому можливість висловлювати свої пригнічені негативні емоції. Наприклад, в реальному житті людина приховує своє невдоволення, заздрість і образу, але не в Інтернеті. Тут вона виплескує весь свій негатив на інших людей і отримує від цього процесу задоволення.

Це основна характеристика людини-троля. Він незадоволений життям, незадоволений людьми, незадоволений собою. Він шукає винних у своїх бідах, а на практиці це виражається так:

1. Будь-яка розмова переводиться на особистості. Троль просто ображає своїх співрозмовників, постійно обзиваючи їх.
2. Сенс розмови зводиться до того, щоб викликати у людини негативну емоційну реакцію. Тролю не важливо предмет розмови. Він отримує задоволення, коли співрозмовник втрачає терпець. Так троль затверджується за рахунок інших.
3. Троль розводить демагогію, демонструючи свої уявні знання з будь-якого питання. Визнати, що він щось не знає - це для нього принизливо.
4. Троль завжди йде проти думки відвідувачів форуму, блогу або соціальної мережі. Здавалося б, це хороша риса, мати свою думку. Однак сенс такої поведінки в тому, щоб створити конфлікт.
5. Троль ставить за мету спровокувати негативну реакцію людей і тому зачіпає в розмові дуже спірні теми. Він любить розмірковувати про політику, про релігію. Йому подобається обговорювати найостанніші події в суспільстві, критикуючи всіх і вся.

Спілкуючись, троль висловлює абсолютну впевненість у своїй перевазі над іншими людьми. Щоб йому не говорили, він завжди правий і до думки своїх співрозмовників не прислухатиметься.

### Як захищатися від тролів?

Знаючи, в чому полягає справжня мета будь-якого троля, не вступати з ним в суперечку або припинити спілкування. Так збережуться час і нерви. За маскою троля, як правило, ховається обмежена людина, якій хочеться розважитися або поповнити свій емоційний резервуар відповідними емоціями. Для троля в Інтернеті ЗАВЖДИ хтось неправий, а його завдання розповісти всім, як хтось в чомусь неправий.

Бувають випадки замовного тролінгу, коли людям платять за тролінг, в тому числі за політичний, але яка б не була причина, щоб уникнути неприємностей, просто їх ігнорувати.

## Фабрики тролів

«Фабрики тролів», що залишають коментарі в соцмережах за завданням урядових структур, діють у 30 країнах. «Фабрики тролів» виявлені в Росії, Мексиці, на Філіппінах, Україні, Білорусії, Малайзії, Марокко, М'янмі, Казахстані, Азербайджані, Китаї, Бахрейні, Ірані і ряді інших держав.

Для українців «фабрика тролів» асоціюється з російською організацією «Агентство Інтернет-досліджень», співробітники якої розміщують в соціальних мережах коментарі на задані теми. Ця організація використовує платних коментаторів для втручання у вибори в іноземних державах, але в основному «фабрики тролів» застосовуються для внутрішніх завдань.

Тролі за гроші у спеціально обладнаних офісах лишають дописи та коментарі, призначені для здійснення російської пропаганди в соціальних мережах, під новинами Інтернет-видань або на інших ресурсах в мережі.

Найняті коментатори з провокативними спотвореними текстовими та графічними повідомленнями стали однією із складових масштабної інформаційної війни Росії проти України з використанням як російських ресурсів, так і ресурсів України, Європи, США, висвітлюючи події в Україні з вигідної точки зору для російської пропаганди.

«Фабрику тролів» задіяли для розміщення політичної реклами в соціальних мережах перед виборами в США і для створення і імітування діяльності різних громадських політичних об'єднань в США.

В 2014 році розпочалась організована кампанія із формування в країнах Заходу про російську збройну агресію проти України. Знайдено документи з інструкціями для коментаторів сайтів Fox News, Huffington Post, The Blaze, Politico и WorldNetDaily.

В них викладено очікуваний об'єм робіт від тролів: в середньому за день вони мають залишати до 50 коментарів до новинних статей. Кожен блогер повинен вести 6 акаунтів у Facebook, публікуючи мінімум 3 записи в день і двічі беручи участь в обговореннях у спільнотах. Інші співробітники повинні вести по 10 акаунтів на Twitter, публікуючи по 50 твітів щодня.

Українські користувачі Facebook зазначають, що проти них діє організована система російських ботів. Вони цілеспрямовано працюють на блокування сторінок відомих українських користувачів соціальної мережі. У 2015 році проблема набула скандалу найвищого рівня. З проханням відкрити офіс Facebook в Україні, який би не залежав від Росії, до Марка Цукерберга звернувся навіть Президент України Петро Порошенко.

### Доксінг

Атака тролів може також містити доксінг. Це відбувається, коли особиста інформація про публічну особу, наприклад адреса або номер телефону, оприлюднюється в Інтернеті. Зазвичай, ця інформація береться з публічних баз даних або з онлайн профілю користувача, але противники можуть також зламати акаунти для отримання особистих даних. Ці дані потім використовуються для переслідування та/або залякування особи, починаючи з оприлюднення матеріалів до погроз по телефону.

## Контрольні запитання

1. Що таке ботнет і як бот може попасти на комп’ютер користувача.
2. Основні ознаки зараження комп'ютера і належності до машин ботнету.
3. Поширені загрози від мережі ботнетів.
4. Як можна захиститися від потрапляння в ботнет.
5. Які функції покладаються на ботів в соціальних мережах.
6. Перелічити поширені різновиди ботів.
7. Типові завдання, які виконують соціальні боти.
8. Які майданчики боти використовують для формування інформаційного впливу.
9. Як можна захиститися від атак тролів
10. Яку мету переслідує доксінг?

## Літературні джерела

1. Що таке ботнет <https://clickfraud.ru/chto-takoe-botnety-i-kak-oni-rabotayut/>
2. Небезпечні ботнети. Приклади загроз <https://vc.ru/services/203285-opasnye-botnety-i-chto-o-nih-izvestno-primery-ugroz>
3. Клік-ферми <https://clickfraud.ru/klik-fermy-chto-eto-takoe-i-dlya-chego-oni-nuzhny/>
4. Що таке боти – визначення і опис <https://www.kaspersky.ru/resource-center/definitions/what-are-bots>
5. Боти в Instagram <https://www.affde.com/ru/instagram-bots-guide-what-marketers-should-know.html>
6. Хто такі лідери думок: класифікація - <https://sendpulse.ua/ru/support/glossary/opinion-leader>
7. Соціальні мережі: тролінг і доксінг <https://rorypecktrust.org/ru/freelance-resources/digital-security/social-media-trolling-and-doxxing/>
8. Бот в соцмережах - <https://ktonanovenkogo.ru/voprosy-i-otvety/bot-chto-ehto-takoe-programmy.html>