Інформаційна безпека під час інформаційної війни

Для волонтерських та ветеранських організацій

Олеся Войтович, Оксана Яцюк
2018

ЗМІСТ

ВСТУП

Сучасне ставлення до інформаційної безпеки можна порівняти з переходом через дорогу у недозволеному місці. Всі знають, що переходити треба на зелене світло, але звичка перебігати на червоне залишилась, і зі словами «мені треба» та «зі мною нічого не трапиться» переходимо на іншу сторону. Все було б чудово, якби сучасні інформаційні технології з маленьких ґрунтових доріг не перетворились на швидкісні багатополосні магістралі, які стає все важче перебігати без ризику для життя..


Інформаційні технології 20 років тому і зараз. Порівняйте ці дві дороги і як їх переходити

При переході ми ще й закриваємо очі, і не бачимо вантажівки, що їде на нас.

Ось так ми ставимося до інформаційної безпеки

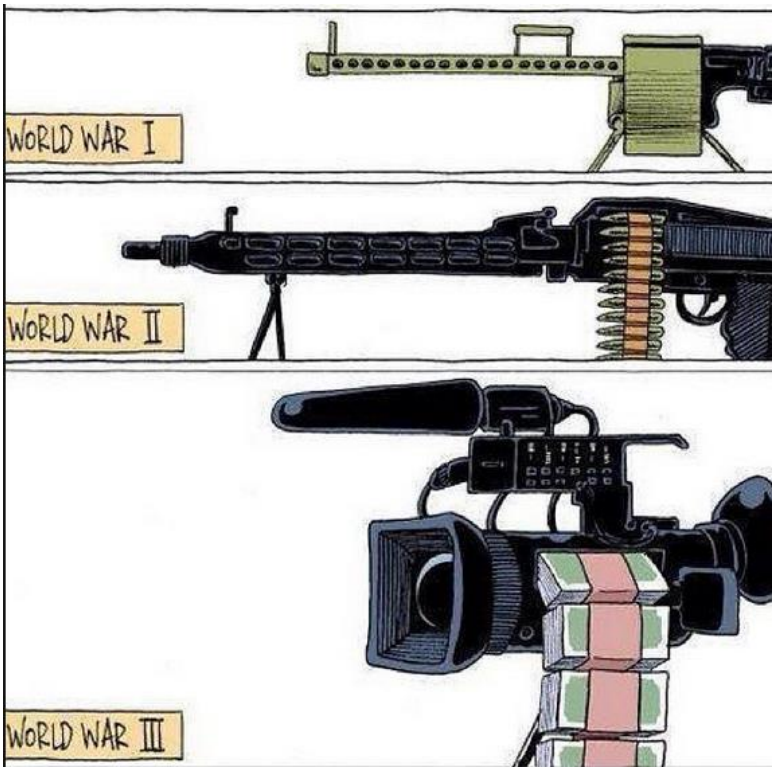
Для того, щоб ефективно протидіяти інформаційним впливам необхідно, в першу чергу, відкрити очі, і навчитися переходити дорогу у відведених місцях.

Задачею цього посібника є навчити людей розумно і раціонально поводити себе під час інформаційної війни, яка проводиться державою-агресором.

А для цього ми розглянемо міфи з інформаційної безпеки і спробуємо їх спростувати.

МІФ 1. ІНФОРМАЦІЙНА ВІЙНА – ТО ВИГАДКА

Шанувальники цього міфу вірять, що інформаційну війну вигадали політики, аби відвернути увагу людей від дій влади.



Насправді

Війни в сучасному світі носять гібридний характер. Їх не оголошують вручаючи ноту і не переходять кордон о 4 ранку. Воюють створенням паніки, розхитуванням внутрішнього конфлікту, кібердиверсіями. Інформаційна війна є складовою частиною сучасних гібридних війн.

Найефективнішою зброєю масового нищення в 21-му столітті буде вже не атомна бомба, якою Росія традиційно лякає світ – а цілком промислові, наразі ще грубі й недосконалі, технології доведення цілих країн до масового божевілля й масового самогубства

Оксана Забужко

ІНФОРМАЦІЙНА ВІЙНА ВЖЕ СЬОГОДНІ

Навіть після анексії Криму дуже мало людей в Україні розуміли, що не треба виглядати російський військовий десант у Києві чи Вінниці, бо він давно захопив наші душі, тільки не через військові аеродроми, а через телебачення та Інтернет, через фільми і серіали, через російську мову на радіо і в ЗМІ. Образно кажучи, росіяни висадились в кожній хаті, де був телевізійний приймач чи комп'ютер, а там, де його не було, вони десантувались через чутки за принципом «із уст в уста».

Основний метод гібридної війни – створити на території держави-противника ситуацію «керованого хаосу», яка призведе до її геополітичного знищення або нейтралізації геополітичних характеристик і держави противника, таких, як територія, економічний потенціал, армія. Важлива роль в гібридній війні відводиться інформаційному прикриттю, діям ЗМІ, які мають приховати від громадян справжню суть акцій керованого хаосу.

Андрій Парубій, 2014

Можна виділити три стадії гібридної війни:

1. Розхитування ситуації, і через кризу створення внутрішнього конфлікту в країні-жертві,

2. Деградація, розорення і розпад країни, поступове перетворенням її в слабку «недієздатну» державу.

3. Зміна політичної влади на цілком підконтрольну агресору.

Зверніть увагу, жодного слова про введення військ чи оголошення війни. Під час гібридної війни, перше – це скоріше допоміжний захід, а друге – взагалі зайве, адже відкритий збройний конфлікт мобілізує населення проти єдиного ворога.

Населення є основним об'єктом гібридної війни, а першочергове її завдання – спонукати громадян зрадити власну державу і стати на бік ворога.

Гібридній війні важко протидіяти, бо вона офіційно не оголошується, ведеться переважно не силами регулярних армії,а силами найманців, або так званих «зелених чоловічків».

Важливу роль грає інформаційний супровід агресії, аби переконати міжнародну спільноту, населення країни-агресора та країни-жертви, що насправді мова йде про внутрішній конфлікт, до якого держава-агресор непричетна. Тому інформаційна війна є невід'ємною частиною гібридної війни.

ІСТОРІЯ ІНФОРМАЦІЙНИХ ВІЙН

Вперше термін «інформаційна війна» вжив в 1967 році колишній директор ЦРУ Ален Далес в книзі «Таємна капітуляція».

Хоча саме поняття «інформаційна війна» з'явилось порівняно недавно, використання інформаційного впливу на ворога практикувалось під час всієї історії людства.

Приклади інформаційного впливу на моральну, духовну стійкість противника можна знайти і біблійних оповідях, і в Давній Греції та Римі, і в пізніші часи.

Особливого значення інформаційні війни набули у XX столітті, коли газети, радіо, а потім і телебачення стали справді засобами масової інформації, а поширювана через них інформація – справді масовою. Уже у 20-х роках минулого століття США вели радіопередачі на регіони своїх «традиційних інтересів» – країни Латинської Америки, Великобританія – на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру – на німців Померанії і Верхньої Сілезії у Польщі, Судетів – у Чехії. Безумовним лідером у використанні інформаційних методів був Радянський Союз, використовуючи радіо, газети, громадські організацій і політичні партії у всьому світі для поширення ідей соціалізму.

Одним з вражаючих прикладів інформаційного впливу на свідомість людей є геноцид у Руанді в 1994 році. Народності хутху і тутсі, які віками жили на цій території, під впливом місцевих ЗМІ перетворились в запеклих ворогів. Протягом кількох місяців було вбито 937 тисяч людей. Швидкість вбивств в 5 разів перевищувала ту, що була в німецьких концтаборах. Провідна газета країни постійно друкувала заклики до вбивства.

Досліджено і доведено роль місцевої радіостанції «Радіо тисячі пагорбів» у масових вбивствах. Зокрема, в тих місцевостях, де мали можливість слухати радіостанцію, кількість вбивць була вищою на 62-69 %. Страхітливі злочини в Руанді свідчать, що ЗМІ не просто віддзеркалює настрої громади, а впливає на

громаду і формує не тільки погляди людей, але і їх поведінку. Міжнародний Гаазький трибунал судив організаторів геноциду в Руанду. Разом з прем'єр-міністром країни до по життєвого ув'язнення були засуджені засновник і директор «Радіо тисячі пагорбів» та редактор провідної газети. 12 років ув'язнення отримав радіоведучий, який закликав до вбивств народу тутсі.

І це фактично єдиний приклад в світовій історії, коли винні у інформаційній війні були покарані.

Починаючи з 2014 р., а особливо з 2016 р. світ зрозумів наскільки небезпечною є інформаційна війна у суспільстві, що фактично повністю покладається на інформаційні технології, і найкращі теоретики та практики намагаються зрозуміти, як її виявляти, як протидіяти, як давати відсіч.

Поява Інтернет і месенджерів практично знищила монополію держав на інформацію (з цим пов'язані спроби багатьох країн ввести обмеження на Інтернет, встановити контроль за трафіком, а також прийняти закони, спрямовані на поширення «помилкових новин»).

Сучасні технології значно розшири засоби впливу як на суспільство, через глобальні технології обміну даними (наприклад, соціальні мережі), так і на інформаційні системи (в тому числі найважливіші, енергетичні або банківські) через Інтернет та мобільні технології. І недарма Дональд Трамп підтримав доктрину застосування зброї у відповідь на інформаційну війну та кібератаки.

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ

На відмінну від традиційної війни, де об'єктами ураження є інфраструктура та ворожа армія, в інформаційній війні – це: свідомість, воля і почуття суспільства; системи управління в політичній, економічній та інших сферах.

Агресію здійснюють, в першу чергу, не війська, а зовнішньополітичні відомства і спецслужби, інформаційно-пропагандистські структури.

Переваги інформаційної війни перед традиційною очевидні. Головна з них – не летальний характер, в ході інформаційних операцій безпосередньо не гинуть люди і військові дії мають другорядне або допоміжне значення. Зникає потреба у військовому вторгненні на територію противника, водночас можна завдавати удару в кількох напрямках.

Війни в двадцятому столітті часто закінчувались судовими процесами, після Нюрберга військові розуміють, що можуть отримати статус злочинців у разі поразки. І в цьому випадку інформаційна війна має свої переваги – матеріальні збитки від інформаційних атак важко довести, виняток – геноцид у

Руанді, в інших ситуаціях практично неможливо притягнути агресора до відповідальності.

Політолог Є. Магда наводить такі переваги інформаційної війни:

- Звичайна війна має відомий і чіткий арсенал дій. Противник відомий. У випадку інформаційної війни можливість передбачити інформаційну атаку майже неможлива, противник часто невідомий, відповідно, відсутня можливість побудувати оборону.
- У звичайній війні територія країни повністю окупована. В інформаційній війні окупація поетапна, проникнення через роботу з місцевими і національними лідерами, молоддю, національними групами. Такі дії можуть відбуватись на тлі загального благополуччя.
- Інформаційна зброя діє вибірково, на різних людей по різному, традиційна зброя діє на всіх однаково.
- На людину одночасно може діяти кілька чинників, які впливають на її свідомість.
- Інформаційна зброя **невидима**. Ознаки руйнівних дій часто відсутні або мало помітні. Населення навіть не відчуває, що на нього впливають. Тому звичні захисні механізми не використовуються, і почуття небезпеки, яке в інших випадках діє миттєво – «почув постріл – тікай», в цьому випадку не спрацьовує. Більше того, люди настільки звикають до інформаційних впливів, що можуть чинити опір спробам побудувати інформаційну оборону, наприклад, відключити трансляцію телевізійних каналів країни-агресора чи обмежити вплив в культурному середовищі.

Інформаційна війна носить неоголошений характер, держава, що її веде, не зізнається в агресивних діях проти іншої держави.

Я все еще доказывала своим родным, от которых ехала в этот день, что результаты этого события не признает никто, поскольку то, что происходит, аж никак не является референдумом. Что все происходит с нарушением всех возможных и невозможных правовых норм. И в России у власти не такие дураки сидят, чтобы подставлять целую страну таким нелепым способом. Мне казалось, любому человеку, который умеет читать и способен прочесть статью словаря «Референдум», это понятно. А уж тем более, людям, у которых высшее образование и пятерки по политологии. Я была уверена, что о присоединении целого полуострова к России за две недели не может быть и речи

Блогер Світлана Паніна

Характерною рисою інформаційної війни можна назвати прагнення агресора безперервно розширювати контрольований інформаційний простір, діючи в обхід моральних норм, і правил, свідомо порушуючи всі соціальні обмеження і моральні установки. Наприклад, інформаційний супровід анексії Криму зі сторони російських ЗМІ дозволив переконати значну частину російських громадян в законності загарбання чужої території і шокувати українських громадян в Криму.

ПІДХОДИ РФ ДО ІНФОРМАЦІЙНОЇ ВІЙНИ

Основним інформаційним агресором проти України зараз є Росія, і багато російських методів ми відчули на практиці. Однак варто звернути увагу на теоретичні основи інформаційної війни, які широко вивчаються в Російській Федерації, а її військові і політичні лідери не приховують свої намірів щодо використання інформації в якості зброї. Причому багато ідей були розроблені та апробовані ще за часів СРСР, проте тоді було ще недостатньо засобів, які б дозволяли провадити їх у життя.

Владислав Сурков відверто пояснив, що ідеальним варіантом для Росії є перетворення конфліктів з високою інтенсивністю у перманентні і довготривалі. Бо при авторитарних режимах постійна мобілізація населення працює на користь владі. При цьому безперервна, але не надто інтенсивна війна може виявитись убивчою для демократії, бо вона роз'їдає усі її базові цінності на чолі зі свободою. Зрозуміло, що для підтримки перманентного конфлікту потрібен потужний інформаційний супровід.

Акцент використовуваних методів протиборства зміщується у бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невоєнних заходів, реалізованих із залученням протестного потенціалу населення. Усе це доповнюється військовими заходами прихованого характеру, в тому числі реалізацією заходів інформаційного протиборства і діями сил спеціальних операцій. До відкритого застосування сили часто під виглядом миротворчої діяльності і кризового врегулювання переходять тільки на якомусь етапі, в основному для досягнення остаточного успіху в конфлікті.

начальник Генерального штабу Збройних сил РФ В.Герасимов
2013 «Военно-промышленный курьер»

В базовій підготовці фахівців силових структур РФ вказано, що

- заходами інформаційної війни є таємні інформаційно-психологічні операції, які здійснюються шляхом керованого інформаційного впливу на індивідуальну, групову або масову свідомість, волю громадян іншої країни, їхні

почуття, дезінформування суб'єктів прийняття політичних, економічних та інших управлінських рішень, здійснення підриву інформаційної інфраструктури противника та ЗМІ цих країн;

- метою є здійснення негативного впливу на свідомість та систему знань і уявлень країни-об'єкту та формування потрібного інформаційного впливу поза її межами;

- бойовим діям повинна передувати здатність забезпечити швидке виведення з ладу інфраструктури політичного та економічного управління противника, а також систем зв'язку та радіоелектронної боротьби;

- створення системи морально-психологічної підготовки військовослужбовців РФ та розробка алгоритмів підриву морального духу противника – вирішальні фактори в сучасній війні.

Об'єктами ураження при цьому визначаються:

- інформаційна інфраструктура держави;

- свідомість, воля та почуття військовослужбовців та різних верств цивільного населення, *особливо у період виборів та кризових ситуацій*;

- системи прийняття управлінських рішень в політичній, економічній, соціальній, науково-технічній сферах та у сфері забезпечення безпеки та оборони країни;

- критично налаштований контингент (опозиція, криміналітет тощо) як засіб посилення кризи в суспільстві.

ЧИННИКИ, ЯКІ СПРИЯЮТЬ ЕФЕКТИВНОСТІ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ

Просто процитую одного вояка.

Нас питають – «за що ми воюєм?». Якщо ми припинимо – ви дізнаєтесь

Волонтерка Лариса Полулях

Геополітична ситуація

Агресивність Росії пов'язана з геополітичним становищем України. Україна перетворилась з ситуативного союзника Росії на жертву російської агресії ще й тому, що гіпотетична поразка України, неминуче вплине не тільки на пост-радянські країни, але і на країни Європи, які перебували під радянським впливом і стали членами ЄС та НАТО.

Відсутність цивілізаційного, інформаційного та фізичного кордону з РФ

Російська імперія та її спадкоємиця Російська Федерація, стверджують фахівці Інформаційного центру «Майдан-Моніторинг», ніколи **не визнавали**

існування українського народу як самостійного, окремого від «державоворчої нації – русских людей». Це невизнання існувало і існує як на рівні державного керівництва, так і в свідомості більшості громадян РФ, і на жаль українців. Навіть серед ліберальної частини громадян РФ переважає концепція про «братські народи» – старший (росіяни) та молодший (українці).

Концепція «братства» українського і російського народів була успішно впроваджена в масову свідомість в совєцькі часи. В постсовєцький період через спільний російськомовний інформаційний простір РФ впроваджувала концепцію «єдиного народу». Станом на осінь 2013 року це призвело до розмиття кордонів ідентичності між українською і російською в східних і південних регіонах України. Взимку 2014 років в інформаційному полі РФ вона отримала назву «Новороссия» з наголосом на штучній «новоросійській» ідентичності з тяглістю до старої імперської.

Великою частиною інформаційної війни РФ проти України є збільшення кількості громадян України, які вважають себе «русскими людьми» або «новороссами», невід'ємною частиною «русского мира». Окупація РФ стала можливою там, де ця мета була досягнена в достатніх обсягах.

Мовне питання

Полегшило російський вплив системне витіснення української мови з України, яке відбувалось з середини 1960-х років. Всюди, крім західних областей, була штучно розвинута залежність від російської мови та сформована уява про меншовартість та «штучність» української мови.

Кордони рускоґо міра – це кордони поширення російської мови.

Людміла Путіна

Ідеологічним обґрунтуванням російської агресії стала концепція «рускоґо міра», як особливо цивілізаційного утворення. В 2000 році Владімір Путін заявив, що поняття «рускій мір» виходить як за межі етносу, так і за межі Російської Федерації. Виступаючи на конференції, присвяченій поширенню російської мови, Людмила Путіна окреслила межі рускоґо міра, а газета «Ізвестия» надрукувала репортаж про її виступ з назвою «Нас 288 мільйонів». Населення Росії на той час налічувало близько 145 мільйонів. До потенційних співвітчизників зарахували російськомовних з інших країн. Логічно, що з часом виникла потреба не тільки нарахувати більшу кількість рускоміровцев, але і фізично приєднати території, на яких вони проживають, до Російської Федерації.

Українська влада довгий час не робила нічого, аби протистояти російській мовній політиці. Агенти Росії активно просували і без того

велетенський вплив російської мови, що проявилось в прийнятті в 2012 році закону «Про основи державної мовної політики» від депутатів Партії регіонів Сергій Ківалова і Вадим Колісніченка. Закон гарантував використання в Україні регіональних мов, тобто мов, які, згідно з даними перепису населення, вважають рідними понад 10% населення, нарівні з державної мовою. На практиці закон означав поділ України за мовною ознакою, і викликав Мовний Майдан.

В лютому 2014 року була спроба відмінити цей закон, що використали російські пропагандисти, як формальний привід для анексії Криму та масових протестних акцій на Донбасі. На сьогодні закон продовжує діяти, і, без сумніву, буде використаний для дестабілізації в Україні.

У Вінницькій області важко зрозуміти масштаби русифікації України, тому поява людей, а особливо дітей, які не знають української мови викликає подив і нерозуміння, так, в Україні справді є люди, які ніколи і ніде не чули української мови. Мовне питання значно ускладнило становище внутрішньо переміщених осіб в Україні, незнання української мови на достатньому рівні і страх мовної дискримінації змушує людей залишатись на окупованій території, часто з загрозою для життя.

Російські, проросійські та російськомовні медіа

Домінування російських медіа – один з чинників, який сприяв успіхові інформаційної війни в Україні. Фахівці з ГО «Майдан Моніторинг» інформують, що після 2000 року керівництво РФ поставило собі за мету досягнення легкої керованості мас через сучасні комунікативні технології – повністю контрольовані і цензуровані телеканали, радіо, друковану продукцію (газети, журнали, книги).

В Україні в 2013 році фактично не існував ринок медіа, найбільш впливові медіа канали були монополізовані олігархами, наближеними до влади. В 2013 році практично весь медійний простір України був заповнений російськомовним продуктом, виробленим у РФ.

Інструментом поширення слугують не тільки окремі активні особи, російське ТБ, але й інформаційні повідомлення, які подаються в друкованій пресі, листівках та передачі місцевих кабельних операторів. Різноманітність чуток змінюється, залежно від ситуації в країні, і цільової групи, на яку вони спрямовані. За чотири роки війни українці «чули» як про зникнення солі в зв'язку з втратою соляних шахт на Донбасі, так і про «небезпечність субсидій», «провал медичної реформи» тощо.

Проросійські інформаційні агентства, видавництва, ІТ-структури, групи блогерів намагаються сформувати деструктивні, панічні, депресивні настрої в

Україні («*нам без Росії нікуди дітися*», «*При владів Україні злочинці*», «*Зрада*» тощо), створити негативний тренд щодо України та одночасно позитивний тренд щодо дій Росії.

Російські Інтернет-сервіси

В 2013 році більшість користувачів Інтернет в Україні користувалася сервісами, повністю контрольованими спецслужбами РФ (mail.ru, vkontakte, одноклассники, антивирус Касперского).

Vkontakte і досі є за замовчуванням соціальною мережею для молоді через більшу розповсюдженість там ігрових і субкультурних спільнот. Поступово і непомітно Vkontakte впливає на українських дітей і молодь через російську мову, відсутність українського контенту, відсутність українських ігор і флеш-мобів.

Релігійні питання

Основною прихованою загрозою є релігійний чинник, зокрема діяльність УПЦ МП в Україні. Священики УПЦ МП, починаючи з анексії Криму, неодноразово в проповідях і виступах підтримували дії російської влади, закликали підтримувати «героїв-ополченців», «священну війну» та боротись з «київською хунтою» не тільки на Донбасі, а й по всій Україні. Своє ставлення до російсько-української війни керівництво УПЦ МП продемонструвало демаршем в стінах Верховної ради, не вставши під час вшанування пам’яті загиблих українських воїнів.

Кібератаки, що провокують паніку та незадоволення владою

Ще у 2004 міністр оборони РФ оголосив про початок розробки програми розширення можливостей здійснення кібервійни та залучення до реалізації цієї стратегії провідних IT-компаній, наукових і навчальних закладів за прикладом США. Російські структури, які здійснюють заходи кібернетичної війни, маскуються під «анонімних хакерів», приватних осіб та організацій («КіберБеркут», Anonymous). За останні роки активність кібератак зростає, і особливо небезпечними вони стали в 2017 році.

За 2014-2015 рр. в Росії було проведено кілька десятків різноманітних конференцій, зустрічей, хакатонів спрямованих на виявлення та експлуатацію вразливостей у обладнанні енергетичних систем А кібератака BlackEnergy на енергетичні системи України сталася у грудні 2015 р., внаслідок чого майже вся Івано-Франківська область залишилась без світла.

Атака на комп’ютерні системи вірусом Petya у 2017 р. породив паніку та зупинила роботу більшості державних та великої кількості комерційних підприємств, відновлення деяких з них продовжується досі.

Акустичне насильство

Одним з нових механізмів впливу на соціальну поведінку, впроваджених СССР та РФ стало аудіо насильство – постійна гучна музика в місцях масового транзиту людей – транспорті, магазинах, ринках та сфері обслуговування. Ця тоталітарна практика досі не усвідомлюється як ненормальна більшістю населення і продовжує відтворюється. Одним з результатів тривалого акустичного насильства стало те, що більшість населення сприймають як норму крик, істеричні і гучні розмови, і не сприймають спокійну розмову, як таку, що варта уваги. Акустичне насильство підсилюють поширені телевізійні ток-шоу, які пропагують крик і перебивання опонента, як норму поведінки.

Зростаючий рівень агресії

Однією з загроз для України є зростаючий рівень агресії, постійно підвищується рівень сприйняття насильства, як єдиного засобу надійного та ефективного вирішення конфліктів. Зростає публічне невдоволення серед активної частини суспільства діями та бездіяльністю державної влади стосовно здійснення структурних реформ та захисту національних інтересів України від агресії РФ. Частково цей стан обумовлений об'єктивними проблемами, а частково є наслідком вдалих диверсійних операцій інформаційної війни РФ.

Бюрократична система,

Не зважаючи на всі зусилля, бюрократична машина, що досталася нам від совєтського минулого ніяк не хоче працювати відповідно до сучасних реалій, і реакція на новітні виклики, в тому числі на інформаційну війну, дуже повільна або взагалі відсутня. А всі спроби активної та свідомої частини суспільства щось змінити тонуть у бюрократичних заморочках.

ПРОТИДІЯ

Усвідомити, що інформаційна війна проти кожного з нас вже ведеться.

Усвідомити, що щоб не відбувалось навколо, Україна має бути понад усе.

Мати власну картину світу і не піддаватися на провокації щодо «руського миру»

Побудувати кордон з РФ – фізичний і цивілазційний.

Пам'ятати, що безпеку, добробут і права людини може гарантувати тільки сильна держава з міцними демократичними інститутами, а не тоталітарний режим.

МІФ 2. КОМУ Я ТРЕБА?

Шанувальники цього міфу вірять, що ворожі інформаційні впливи спрямовані винятково на впливових і заможних людей. Звичайні люди, які не займають високих посад, не керують великим бізнесом, можуть бути спокійними – вони нікому не треба.

Насправді

Он угостил меня кофе, печенькой. И в конце сказал: «Мы же с вами люди маленькие».

Я поперхнулась: «Вы со мной, пожалуйста, в один ряд не становитесь. Вы читали основание в отказе на въезд – я могу угрожать обороноспособности самой Российской Федерации. А вы? Вы на что влияете?»

Анастасия Рингис, Четыре года запрета на въезд домой (діалог української журналістки і працівника ФСБ Росії на в'їзді в Крим в 2016 р.)

Інформаційний вплив спрямований на все населення країни. Всі люди є під загрозою.

ЛЮДСЬКИЙ ФАКТОР

Головна проблема безпеки – це людський фактор

Кевін Мітнік, визначний хакер

Майже 70% *успішних атак пов'язані з людиною.* Symantec.

Мета інформаційної війни
– це свідомість (душі) людей, а не ресурси.
– створити цілісну картину світу, де стають виправданими багато дій та вчинки, які ніколи б не були зрозумілі і виправдані поза цією картиною.

Найважливішими мішенями для ворожих інформаційних впливів є ветерани і волонтери, які по суті залишаються активною частиною суспільства, що бореться за інтереси нашої держави:

- саме волонтерська спільнота зіграла вирішальну роль у збереженні української державності в 2014 році, коли державні структури були паралізовані, а армія – зруйнована;
- ветеранські організацій мають серйозним вплив на всеукраїнському і регіональному рівнях, і політичні сили змагаються за контроль над ними;
- згідно з опитуваннями, волонтери є одними з найбільш авторитетних інститутів в Україні і мають високий рівень довіри в громадян. Тому ворог намагається зменшити їх вплив через методи інформаційної війни.

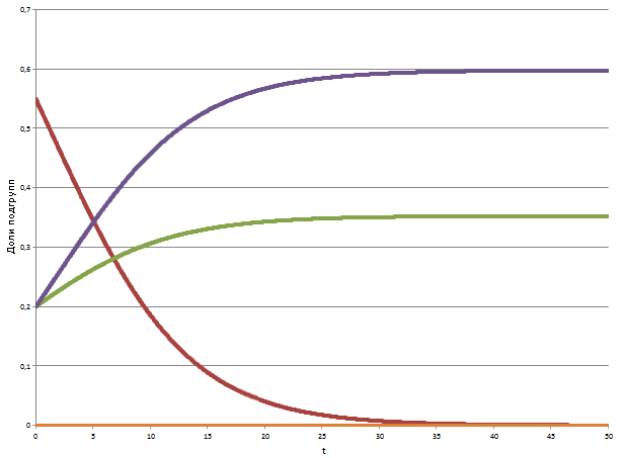
Інформаційна війна – є електронним конфліктом, де інформація є стратегічним здобутком, який варто захопити чи знищити. І комп'ютери, і інформаційні системи стають привабливим напрямком першого удару

Уін Швартоу, США 1997

Кому ж потрібні «звичайні» люди?

- фінансовим шахраям, які різними способами видурюють у людей гроші;
- продавцям товарів і послуг – їм потрібні клієнти;
- політикам, які полюють на голоси виборців;
- **ворожим силам** з Росії – цим потрібне все, перераховане вище: ваші гроші, ваше майно, ваші голоси на виборах, ваша свідомість і ваші переконання, все, що схилить людей зрадити свою державу і перейти на бік ворога. Потенційні зрадники потрібні ворогу на різних рівнях, від бурмотіння «все погано» у громадському транспорті до прийняття шкідливих для країни рішень державними службовцями.

Інформаційну війну можна порівняти з епідемією інфекційної хвороби. Заможна людина чи бідна, займає вона високу посаду чи працює за мінімальну зарплату на півставки – в сезон епідемії шанси захворіти є у всіх. В кращій ситуації ті, хто подбав про щеплення, але і вони під загрозою, якщо виявиться, що вірус не той, на якого сподівались.



Модель розвитку вірусних епідемій

На малюнку можна побачити модель розвитку вірусних епідемій, де червона лінія – здорові, зелена і синя – ті, хто захворів на штами з різною здатністю до зараження.

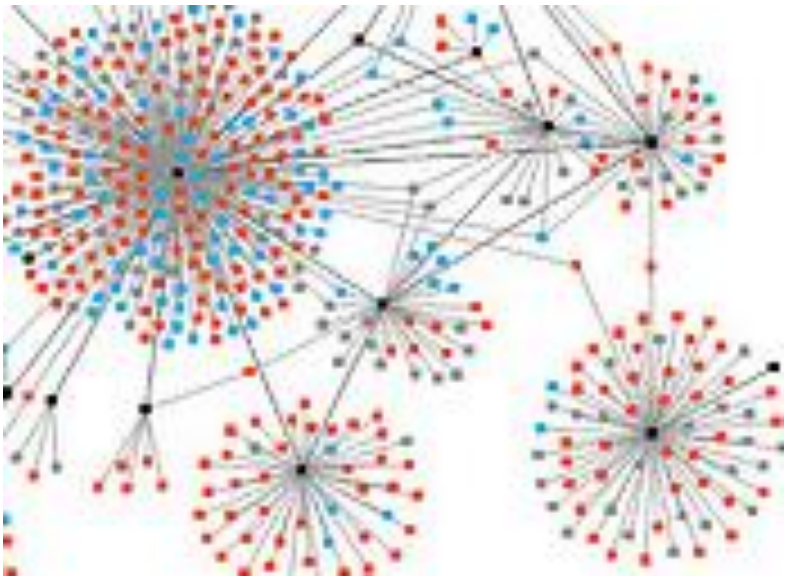
.

Майже така сама модель описує зміну думки ізольованої спільноти (кластера) під дією інформаційного впливу. Якщо набирається певна кількість заражених осіб (так звана точка біфуркації), процес вже не зупиниться без додаткового зовнішнього впливу і спільнота стане зараженою інформаційним вірусом.

СОЦІАЛЬНІ ПОСЕРЕДНИКИ І КЛАСТЕРНЕ СУСПІЛЬСТВО

Інформація в українському суспільстві поширюється і функціонує всередині кластерів, (співтовариств, громад, спільнот), які об'єднують людей за принципом «подібне до подібного». Наприклад, шанувальники здорового способу життя і домашньої освіти утворюють один кластер, а любителі пива і чіпсів – інший. Вірні різних церков і атеїсти всіх напрямків інформаційно об'єднуються зі своїми однодумцями.

Всередині кластерів циркулюють інформаційні повідомлення, але кластери достатньо ізольовані одне від одного, і те, що обговорюють в католицькій громаді, не дійде до православної. Не через секретність інформації, а швидше через неважливість її для іншого кластеру. В кожному кластері є група людей, думка яких більш авторитетна, до них частіше звертаються, вони мають більше зв'язків. Таких людей називають інформаційними вузлами.



Візуалізація кластерів у суспільстві

Людина-інформвузол не обов'язково є експертом з якихось питань, але вона вміє створити навколо себе комфортне середовище, їй довіряють і охоче спілкуються. Через свої комунікаційні здібності такі люди отримують багато інформації від інших. Цю інформацію вони перетворюють у зрозумілі для свого оточення форми і поширюють у своїй спільноті. Інший тип людей, соціальні

посередники, підтримують зв'язки між кількома кластерами. Вони передають інформацію для вузлів, які поширюють далі.

Незалежно від ролі людини в кластері – звичайний учасник чи вузол/посередник, кожного чи кожну можна використати для інформаційного впливу. Учасники можуть передавати інформацію для вузлів чи посередників, а ті – розповсюджувати її в своєму оточенні.

Роль вузлів в ситуації сучасної України виконують громадські активісти і волонтери!

Ольга Малишева

Люди, що підтримують зв'язок між двома або кількома кластерами – **соціальні посередники** – є носіями унікальної інформації, яка становить інтерес для вузлів, а за їх посередництвом буде донесена і до решти. В деяких випадках соціальний посередник може стати центральним вузлом для декількох кластерів, а може залишатися просто ланкою.

При виборі мішені інформаційно-психологічної операції зловмисники отримують найкращі результаті, впливаючи на соціальних посередників, адже вони можуть передавати та інтерпретувати меми (повідомлення) у декілька кластерів, формуючи думку великої кількості людей. Проте впливати на соціальних посередників важко, бо вони здатні аналізувати та робити висновки, а отже, саме соціальних посередників найчастіше намагаються вивести з інформаційної мережі (в тому числі і фізично або дискредитуючи через чорні технології).

Легше впливати на осіб, що є вузлами мережі. Як і будь-яку людину, їх обманюють, маніпулюють чи перекуповують. Спільнота по-різному реагує на зміну думки інформаційного вузла. Перший сценарій, коли, внаслідок зміни думки вузла лавиноподібно змінюється думка людей в оточенні. Другий – коли вузол дискредитований, і на його повідомлення більше не звертають увагу. Третій, коли внаслідок внутрішніх протиріч спільнота руйнується. У всіх трьох випадках порушується стійкість спільноти, що робить її вразливої для наступних інформаційних впливів .

Найлегше впливати на окремих членів спільноти. Якщо охопити достатню кількість таких «звичайних» людей, вони впливатимуть на весь кластер. Крім того при зараженні окремих учасників кластеру, можна сподіватися, що епідемія «захопить» і людину-вузол мережі. Тоді розвиток подій відбудеться за першим сценарієм.

ДОСТУП ДО ІНФОРМАЦІЇ

Кожен з нас є учасником, вузлом або посередником, або те і те у суспільстві, залежно від характеру, роботи, харизми, випадковості тощо.

І кожен з нас має інформацію, що може дозволити провести інформаційну операцію проти нас, або проти інших вузлів кластеру, або проти всього суспільства.

«Інформація – це нафта сучасного світу»

«Хто володіє інформацією, той володіє світом»

Ці тези знають багато людей, але чи всі розуміють цінність інформації, що їх оточує? Напевно, ні.

*Інформація – це **нові** дані, які дозволяють приймати рішення та керувати системою*

Теорія систем

Відповідно до теорії систем, цінність інформації визначається її новизною. Якщо людина (система) щось знає, це не є вартісним, а отже не потребує збереження. Що знаєш – часто не цінується, а що не цінується – не бережеться.

Але якщо інформація є новою, раніше невідомою, то вона має велику вартість, і для її отримання витрачаються великі ресурси (часові, матеріальні, людські).

Ось в чому парадокс! Одна й та ж інформація для когось є відомою, а для когось – ні. В першому випадку вона нічого не варта, а в другому – купується за мільйони.

Наприклад – дата народження. Чи зберігає хтось в таємниці ці дані? (Ми не говоримо про агентів спецслужб.) Точно – ні. А який пароль від WiFi ви використовуєте? Чи не дату народження? Ось і виходить, що для вас дата народження не є цінністю, що варто зберігати, а для вашого сусіда – дуже корисна інформація, що дозволяє зекономити на оплаті рахунків.

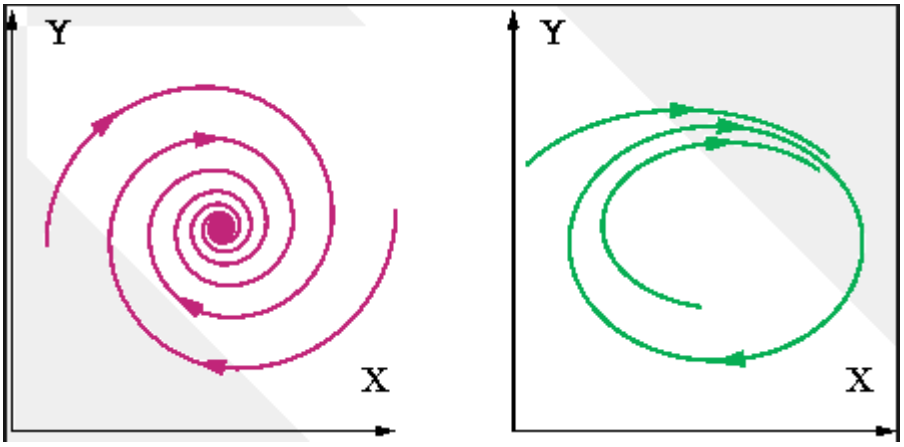
ЕФЕКТ МЕТЕЛИКА

«Помах крил метелика в Бразилії викличе торнадо в штаті Техас»

Едвард Лоренц

Ефект метелика – термін у природничих науках. Він означає, що незначний вплив на систему може мати великі і непередбачувані ефекти де-небудь в іншому місці і в інший час.

Одна й таж сама система (біологічна, технічна чи соціальна) при різних початкових умовах впливу може або повернуться у початковий стійкий стан і далі функціонувати, або перейти у нестійкий стан і породжувати кризу за кризою.



Модель «ефекту метелики»

До чого тут інформаційна війна і позиція окремої людини?

Думка навіть однієї людини може кардинально змінити ситуацію навколо. Активні люди змінюють українське суспільство. Майдан, допомога армії, порятунок безпритульних тварин, сортування сміття – ці рухи почались з ініціативи кількох людей, а вплинули – на всю Україну.

Якщо хоча б одна людина бачить «вантажівку», що їде назустріч, вона може «відкрити очі» іншим.

ПРОТИДІЯ

Припиніть вважати себе нікому не потрібними «звичайними людьми».

Усвідомте реальність інформаційної війни і дбайте про власну інформаційну безпеку.

Свідомо ставтесь до власних слів і вчинків, пам’ятайте про можливий вплив на спільноту.

Дочитайте цей посібник до кінця та виконуйте рекомендації.

МІФ 3. НІХТО ПРО МЕНЕ НІЧОГО НЕ ЗНАЄ

Люди, які вірять в цей міф, вважають, що про їхнє життя, звички, статки нічого не відомо. І ніхто не зможе про це дізнатись, аж доки вони самі не напишуть докладну автобіографію в одному примірнику і від руки. Люди впевнені, що інформація, яку вони надають державним і приватним структурам, викладають в Інтернет, згадують в приватному листуванні в соціальних мережах – залишиться конфіденційною і недоступною для інших.

Міф 3. Ніхто про мене нічого не знає

Насправді

Дані про людей, їх дії і навіть наміри зберігаються і накопичуються в мобільних пристроях, соціальних мережах, державних та приватних реєстрах.

Користуючись навігаторами ми залишаємо інформацією про свій маршрут.

Викладаючи особисті фотознімки в соціальних мережах ми інформуємо всіх бажаючих про свою родину, роботу і дозвілля.

Шукаючи товари і послуги через пошукові системи ми залишаємо інформацію про власні потреби і вподобання для рекламістів і маркетологів.

Скільки зберігаються ці дані? Невідомо. Користувачі не контролюють тривалість збереження даних про себе. Навіть якщо ви видалите профіль з соціальної мережі або розірвете договір з банком – дані про вас зберігатимуться і можуть бути використані вам на шкоду.

Витік даних трапляється з різноманітних систем, про які звичайний користувач навіть не замислюється. Ось невелика підбірка витоків даних за 2017-2018 р.

Uber заплатив $100 тис. за видалення даних про 57 млн. користувачів.
Витік про 400 тис. клієнтів UniCredit.
Dow Jones помилково опублікував дані про 2,2 млн. клієнтів.
Особисті дані 14 млн. клієнтів Verizon виявились у відкритому доступі.
Хакери опублікували 25 тис. фото пацієнтів клініки пластичної хірургії.
На продаж виставлено 25 млн. логінів Gmail з паролями.
У знайденій флешці були дані про системи безпеки аеропорту Хітроу.
Китайські хакери викрали найновіші розробки американських ВМФ.
Клієнти канадських банків стали жертвами витоку даних.

Спеціалісти з безпеки зафіксували в першій половині 2017 року витоки 7,78 млрд записів із персональними та платіжними даними по всьому світу.

В цих списках відсутні українські бази даних. Але це лише особливості українського законодавства, яке не вимагає обов'язкового оприлюднення інформації про витоки даних.

Життя сучасної людини важко уявити без Інтернету. Електронне листування, перемовини через скайп, соціальні мережі є невід'ємною частиною щоденної рутини. Через Інтернет спілкуємось з родичами і колегами, оплачуємо послуги, шукаємо матеріали для навчання, просто проводимо вільний час за переглядом цікавих роликів. Багато людей вважають цю

ситуацію цілком безпечною і навіть не замислюються, як перебування в мережі може їм зашкодити.

РЕЄСТРИ ВІДКРИТИХ ДАНИХ

З 2015 року в Україні активно розвивається сфера відкритих даних (OpenData). Держава Наприкінці грудня 2017 р. уряд схвалив оновлену постанову №835, яка розширює кількість наборів даних до 600 та покращує норми щодо їх оприлюднення у формі відкритих даних.

Список відкритих реєстрів та наборів даних можна подивитись на єдиному державному веб-порталі відкритих даних http://data.gov.ua/. Існує багато недержавних реєстрів.

Однією з умов використання відкритих даних є деперсоналізація, проте можна зібрати інформацію і по конкретним підприємствам та людям.

Ринок відкритих даних стрімко розвивається в Україні та в усьому світі. В цьому немає нічого кримінального та незаконного. Провідні компанії світу і маленькі стартапи зацікавлені у відкритих даних. Це можливість відстежити тенденції та явища, слідкувати за виконанням законів (наприклад реєстр безкоштовних ліків), боротися з бюрократами та знаходити вільні земельні ділянки, перевіряти надійність партнерів та організацій, екологічний стан довкілля тощо.

Open data від YouControl: безкоштовне досьє на кожну компанію з 22 держреєстрів

Проте існує багато застережень. Наприклад, в реєстрі нерухомості можна побачити, хто якою нерухомістю володіє, а в базі електронних декларацій – хто скільки заробляє.

Будь-яка людина може раптом опинитися у центрі шахрайської схеми, яка будується на даних з відкритих реєстрів, прямих чи опосередкованих. І, на жаль, далеко не кожна людина розуміє, що багато її даних просто так знаходяться у відкритому доступі та можуть бути використані проти неї.

ДЕРЖАВНІ РЕЄСТРИ

Хоча багато реєстрів є відкритими, все ж залишаються дані, захист яких гарантує держава.

- Державна фіскальна служба,
- Пенсійний фонд,
- Державна міграційна служба,
- МВС,

- реєстр персональних ідентифікаційних кодів фізичних осіб,
- реєстр перетину товарів державної кордону митної служби,
- реєстр транспортних засобів,
- реєстр інформації Національної поліції України,
- реєстр земельного кадастру України,
- реєстри виборців,
- та інші.

Частина даних з цих реєстрів може бути відкрита, але частина залишається конфіденційною, це персональні дані, дані про національні інтереси чи державну таємницю. Наприклад, факт дорожньої аварії є відкритою інформацією, а прізвища учасників та особливості розслідування – закритою.

Державні реєстри суворо охороняються, проте, як і всюди у світі, трапляються витоки. Розповідають, що база даних реєстрів виборців спочатку з'явилась на «Петрівці» (великий книжковий ринок у Києві), а потім вже у виборчих комісіях. Цей факт не можна ні підтвердити, ні спростувати, бо в Україні відсутнє законодавство, яке зобов'язує оприлюднювати інформацію про витік баз даних.

ПРИВАТНІ РЕСУРСИ

Крім державних реєстрів, існує велика кількість приватних ресурсів, в яких міститься багато інформації, що може бути використана. Це бази даних:

- операторів мобільного зв'язку;
- провайдери Інтернет;
- кредиторів;
- перевізників, в тому числі Укрзалізниці;
- платіжних систем;
- електронних магазинів;
- різноманітних гаджетів;
- тощо.

До цих ресурсів не висуваються вимоги стійкого захисту (наприклад дані з фітнес-браслетів передавалися і зберігалися у відкритому вигляді, а за їх аналізом вдалося відстежити шлях людини з точністю до кількох сантиметрів).

Місцезнаходження секретних американських баз стало надбанням громадськості. Компанія-розробник фітнес-додатків для бігу опублікувала карту, яка допомогла розкрити місце знаходження військових баз і маршрути патрулів кількох армій світу, як американських, так і турецьких чи російських.

Навіть, якщо вимоги безпеки виконуються, доступ до даних можуть отримати як представники МВС та спецслужб, так і просто «знайомі» операторів цих систем.

Крім того, існує незаконна практика обміну даними між різними ресурсами, що дозволяє приватним медичним закладам знати, чи отримує людина субсидію, а банківським установам дзвонити пенсіонерам та пропонувати переходити на обслуговування у їх банк.

БАНКІВСЬКІ СИСТЕМИ

– Чому Ви звернулись саме до мене? Як Ви дізнались?

– Мені підказав одногрупник.

– Але де ж Ви взяли мій номер телефону? А, напевне, у Вас є спеціальні бази даних.

– Ні. В мене знайомі у ПростоБанку…

Розмова з кіберполіцейським

Як і державні та інші ресурси, банківські системи викликають суперечливе ставлення. З одного боку суспільство ще пам’ятає стереотип про надійні швейцарські банки і їх ставлення до таємниці, з іншого щоденно люди стикаються з повною безвідповідальністю банківських працівників.

Прикладів можна наводити багато. Працівниця банку розповідала, що пін-код від карти – не така вже й таємниця, і вона повідомляє свій пін-код продавцям у супермаркеті, щоб не вводити власноруч. А якщо потрібно дізнатися номер телефону особи (адресу тощо), достатньо мати «друга» у банку.

Кількість даних, що зберігається у банках, величезна. Крім даних, які користувач безпосередньо повідомляє у банк, там накопичується й інша інформація: отримання коштів (зарплата, пенсія, соціальні платежі), витрати (комуналка, магазини, електронні портали, де йде розрахунок через карту банку). Аналіз такої інформації може стати «золотим дном» для аналітика.

Сбербанк РФ з 2018 р. починає використовувати «психологічний скорінг» для оцінювання кредитоспроможності клієнтів. Спеціальна програму буде аналізувати, що лайкає, коментує та читає потенційний зйомник, для створення його психологічного портрету, і далі спеціалісти банку будуть приймати рішення щодо кредиту.

Хоча банківські установи повинні дотримуватись високих стандартів безпеки, багато українських банків, навіть топових, не проходять міжнародних сертифікацій з безпеки. І тут вже не спишеш на нестачу коштів.

МОБІЛЬНІ ПРИСТРОЇ

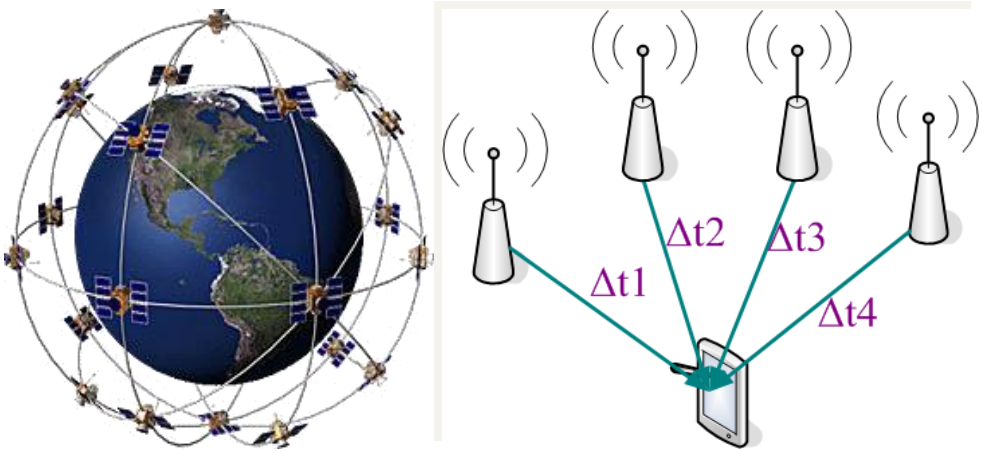
Найпоширеніші області застосування мобільних пристроїв у звичайному житті – це ведення списку контактів (друзі, знайомі, колеги), соціальні мережі, ігри, робота з поштою, веб-серфінг, ведення електронного щоденника, здійснення покупок в Інтернет, робота з фото, відео, формування маршрутів тощо.

Дані з пам'яті пристрою

Користувачі записують на смартфон власні персональні дані або інформацію своїх друзів і колег. Логін і пароль (часто занесені у пам'ять), доступ до поштових скриньок, соціальних мереж, інтернет-банкінгу, електронних кабінетів. Витік такої інформації може призвести не тільки до розголошення суто приватних відомостей, але й до прямих фінансових втрат. Крадуть не тільки гроші, а й облікові записів у соціальних мережах для використання у інформаційній війні.

Дані GPS

Суттєвим джерелом витоку може стати GPS-модуль, встановлений у кожному мобільному пристрої. Він допомагає орієнтуватись у просторі, бачити, де знаходишся, отримувати додаткову інформацію. Водночас він є джерелом інформації про місцезнаходження з дуже великою точністю. На кожній зробленій фотографії чи знятому відео при включенні GPS формується тег з координатами. Точність тегу – від кількох метрів до кількох сантиметрів. Додатки соціальних мереж підтягують дані з GPS, і всім друзям (і не тільки) можуть показати, що зараз людина у ресторані в Єгипті або на мітингу з підтримки політичного діяча.



Схематичні зображення системи GPS

Багато мобільних додатків зберігають історію переміщень і діляться нею як з виробником додатку, так і третьою стороною (наприклад, рекламною агенцією).

Шпигунські програми

Через специфіку роботи більшість мобільних пристроїв є вразливими для шпигунського програмного забезпечення. В першу чергу через те, що людина не читає та не звертає увагу на дозволи, власноруч надані тій чи іншій програмі, сподіваючись на попередню перевірку адміністраторів майданчику /платформи/мережі або сповідуючи міф 2.

Зараження через Google Playmarket у 2017 р. становить 0,005% (і це тільки офіційні дані). Кількість скачувань – десятки та сотні мільярдів. Кількість заражень – сотні тисяч.

Виробники шпигунських програм настільки впевнені, що ніхто не читає їх ліцензійні умови, що почали відкрито інформувати про можливість передачі даних. «Дані користувачів будуть збиратися, оброблятися та передаватися третім особам», – пишуть в угоді, але хто читає ці угоди?

Потрапляючи в систему, шпигунська програма завдяки правам, що надані самим користувачем, може майже все:

- слухати розмови;
- записувати, що говорять навколо;
- робити фото- та відеознімання;
- копіювати дані з пам’яті смартфону (контакти, смс, історію телефонних дзвінків, серфінг у мережі, логіни та паролі..);
- робити скріншоти з екрану (наприклад, щоб перехопити спілкування у месенджерах);
- збирати характеристики телефону та про інші встановлені додатки;
- фіксувати місцезнаходження;
- передавати зібрані дані розробнику або замовнику для подальшої обробки та аналізу через різноманітні канали зв’язку.

ДАНІ ПРОВАЙДЕРІВ

У більшості країн світу від операторів зв’язку (стаціонарного, мобільного, Інтернет тощо) вимагають мати обладнання для прослуховування трафіку, що йде через цього оператора. В деяких країнах доступ можливий лише за рішенням судів (ФРН), а в деяких – за прямим доступом агента ФСБ (РФ). В

Україні вже є закони, що вимагають від провайдерів встановлювати відповідне обладнання, але докладна процедура прослуховування всіх ще не прописана.

Це не означає, що в Україні неможливо отримувати дані від провайдера, як законним, так і не законним шляхом.

Можна легко отримати:

- інформацію про дзвінки за тривалий період;
- інформацію та вміст смс;
- місцезнаходження та переміщення мобільного телефону (з точністю від кількох метрів до сектору базової станції).

Трохи складнішою задачею є

- прослуховування розмов;
- втручання у розмови.

При використанні користувачем послуг мобільного зв’язку (2,3,4 G) можна дізнатися обсяг трафіку, відвідані веб-сторінки тощо.

Жартівливе фото з Укртелекому

Функції підслуховування та перехоплення вже вбудовані в обладнання операторів. За найпростішими алгоритмами відфільтровується інформація за номером, за абонентом, за пристроєм (якщо міняють сім-карту), складніші алгоритми дозволяють аналізувати за голосом, за ключовими словами.

Може досліджуватись весь трафік абонента: відвідування сайтів, зіставлення відвідувань сайтів, MAC- і IP-адрес, даних геолокації і мобільних вишок. Так встановлюється зв'язок між різними пристроями однієї людини, відстежується переміщення і встановлюється адресу проживання, місце роботи, справжнє ім'я і багато іншого, навіть якщо вживаються заходи щодо анонімізації.

ДАНІ З КАНАЛІВ ЗВ'ЯЗКУ

Перехопити і прослухати на сьогоднішній день можна всі (або майже всі) канали зв'язку.

Стаціонарний телефон

Вже майже ніхто не використовує звичайний проводовий телефон.

І не останню роль тут зіграла майже повна відсутність механізмів захисту інформації від прослуховування. Телефонні мережі прослуховуються досить легко, з 80-х рр. минулого століття схеми прослуховування публікувались навіть у журналах на кшталт «Юний техник», не говорячи про спеціалізовані видання.

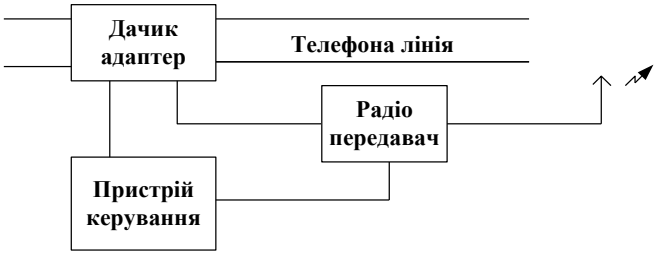


Схема підслуховуючого пристрою

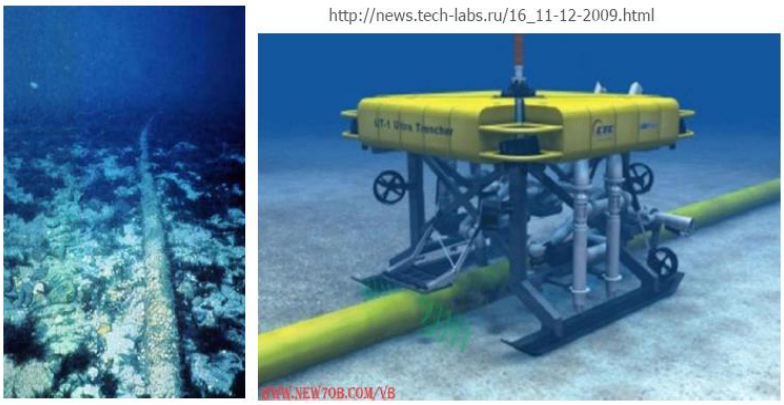
Побудувати ефективні системи захисту в цьому випадку майже неможливо. Крім прослуховування безпосередньо розмов «по телефону», можна прослуховувати і розмови, що ведуться у приміщення, і навіть там, де є дроти телефонної лінії.

Проводовий Інтернет

Для обміну даними інтенсивно використовуються проводові лінії зв'язку (ATM, Ethernet, оптоволокно). І ці канали зв'язку мають свої вразливі місця, які дозволяють зловмисникам так чи інакше підключатися і перехоплювати трафік.

Ваш сусід може підключитись до роутера, або поставить спліттер (пристрій для дублювання трафіку, що передається каналом зв'язку), а можуть бути спецслужби, які прослуховують і аналізують весь трафік у магістральних каналах.

Особливістю Інтернет-зв'язку є те, що навіть коли зв'язок відбувається між двома сусідніми комп'ютерами, трафік може йти через Київ, або Москву або Амстердам, або іншим шляхом, залежно від дуже багатьох технічних і не дужу причин. Тому можна сидіти в Амстердамі і отримувати всю необхідну інформацію про трафік у Вінниці. Технологічно це навіть не дуже складно.



Магістральний інтернет-кабель та підключення до нього

Безпроводові канали зв'язку

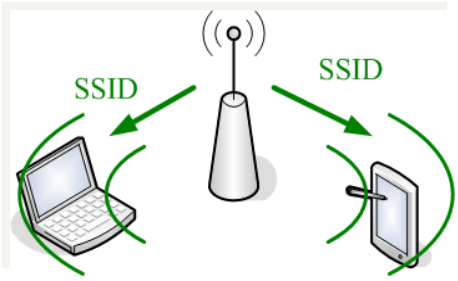
Потенційно небезпечні зовнішні канали передачі даних Wi-Fi і Bluetooth. При виході в Інтернет через ці канали трафік користувача може бути адресований на підроблений або шкідливий сайт, хакерську точку тощо.

Бездротові мережі використовують радіохвилі. Ефір – середовище з загальним доступом і практично повною відсутністю контролю. Таким чином, мережа стає доступною з іншого поверху або навіть з сусіднього будинку, парковки або іншого кінця вулиці – радіосигнал може поширюватися на сотні метрів за межі будівлі. Єдиною фізичною межею бездротової мережі є рівень цього самого сигналу.

Тому, на відміну від провідних мереж, в бездротових мережах підключитися можна звідки завгодно, аби сигнал був достатньої сили. Будь-який бездротовий пристрій може «бачити» всіх бездротових сусідів в мережі, а сам залишатися невидимим.

Ще більшою проблемою є мобільність бездротових користувачів. Вони можуть з'являтися і зникати, змінювати своє місце розташування, перебувати де завгодно в зоні покриття.

Фактично захиститися від прослуховування бездротових мереж неможливо.



Точка доступу Wi-Fi та пристрої, що до неї підключаються

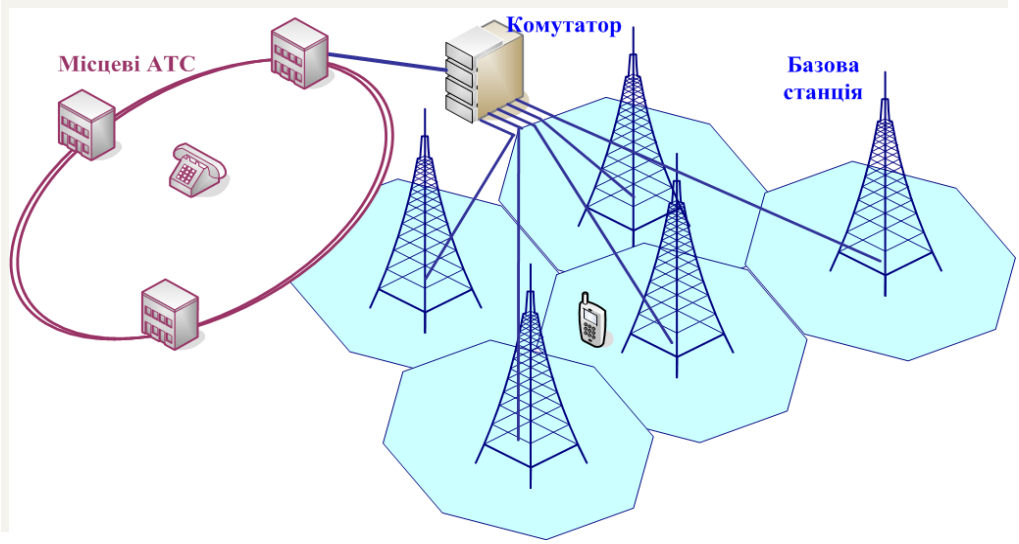
Такі технології бездротового зв'язку як Wi-Fi і Bluetooth на сьогоднішній момент є найбільш вразливими. Вони не мають сильних механізмів захисту, а ті що існують, вже взламані. Для зловмисника отримати дані, що передаються

цими каналами, навіть захищеними, питання від кількох хвилин до кількох тижнів, залежно від обладнання.

Крім того зловмисник може підробити точку доступу, і не тільки копіювати дані, але й змінювати передані дані. Так кожного разу, коли ви приєднуєтьсь до WiFi, ви ніколи не можете бути впевненими, у справжності цієї точки доступу, і що дані, які ви отримуєте не є підробленими.

Мобільні канали зв'язку

На відміну від інших каналів зв'язку, GSM та CDMA мають вбудовані механізми захисту, які були досить потужними на момент їх створення. Але з того часу технології прослуховування вдосконалились.



Узагальнена схема мобільного зв'язку

Кілька років тому було оприлюднено дані вразливість всіх систем мобільного зв'язку. Вона дозволяє при певному обладнанні та програмному забезпеченні не тільки прослуховувати розмови, (незалежно від провайдерів, місцезнаходження, країни), але й в режимі реального часу втручатися в розмову. Вартість такої системи обчислюється десятками мільйонів доларів, але хіба це гроші, коли мова йде про національні інтереси чи інформаційні війни?

РОЗУМНІ РЕЧІ

За останні кілька років наш світ доповнили так звані «розумні речі» та «розумні будинки». Ця новітня технологія фактично означає, що будь-якій «розумний пристрій», холодильник, кавоварка, телевізор, праска тощо має вихід в Інтернет і може як передавати, так і отримувати дані та команди, обмінюватись інформацією з іншими розумними пристроями та приймати рішення. Наприклад, кавоварка підключається до Інтернет та сама шукає нові

рецепти приготування кави, залежно від того, що є холодильнику або радіо-няня фіксує коли дитина проснулась, робить фото і направляє їх на смартфон.

Проте нова технологія породжує нові ризики.

Веб-камери можуть спостерігати за всім, що відбувається в них, розумні телевізори можуть записувати звук та відео, розумний автомобіль може інформувати, коли його власник дома, а розумна праска розсилати спам.

Коли ви дивитись телевізор, телевізор дивиться на вас

А хто надає команди вашим розумним пристроям ? Невідомо.

ПРОТИДІЯ

Пам’ятайте, що ваші дані є в різних сховищах і можуть бути використані:

- шахраями;
- зловмисниками;
- ворожими агентами.

Вимикайте за замовчуванням канали зв’язку, які ви не використовуєте.

Відключайте GPS-модуль, якщо його не використовуєте для навігації в даний момент.

Перед розміщенням фото та відео у мережі (чи навіть на власному комп’ютері), зачищайте геодані (наприклад, перезбережіть через графічний редактор).

Використовуйте тільки захищені канали зв’язку.

Не користуйтесь публічними мережами (відкритий WiFi).

Використовуйте VPN при використанні WiFi та Bluetooth.

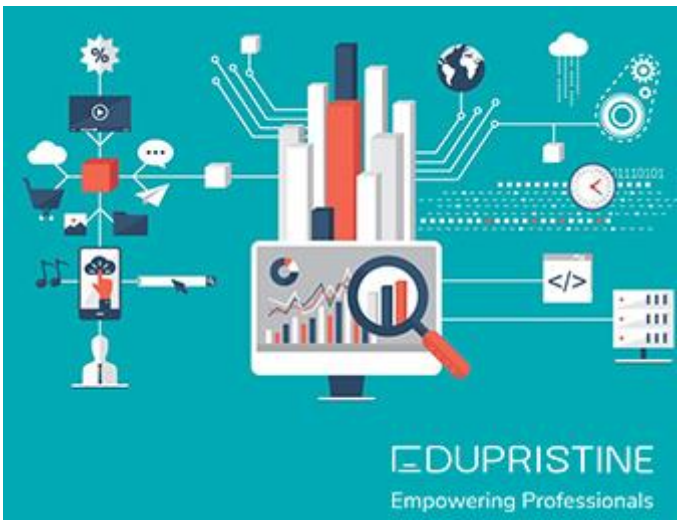
Не сподівайтесь на захищеність мобільного зв’язку.

Пам’ятайте, що сучасні «розумні речі» недосконалі з точки зору безпеки і можуть бути використані проти вас.

Вимагайте законодавчого обмеження терміну зберігання і використання ваших даних у державних та приватних реєстрах.

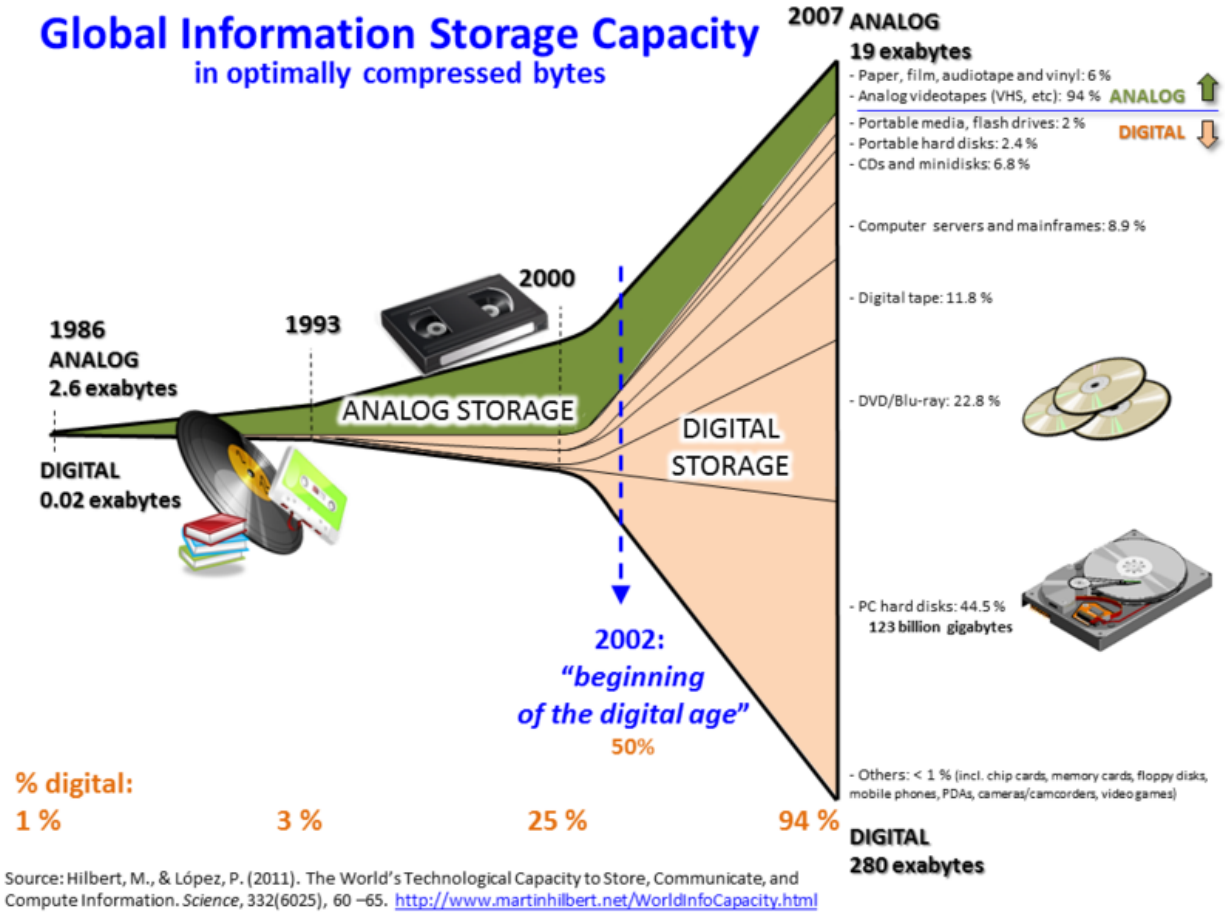
МІФ 4.
ПРОАНАЛІЗУВАТИ ДАНІ ПРО ВСІХ – НЕМОЖЛИВО

Гаразд, наші данні зберігаються, вважають шанувальники цього міфу, але проаналізувати їх – неможливо. Об'єм інформації надто великий і у світі не знайдеться стільки дослідників.



Насправді

Такий підхід мав місце у минулому, коли дані зберігалися у аналоговій формі. Дані накопичувались, проте людей, що здатні їх проаналізувати не вистачало, оброблялась інформація тільки за найвищим пріоритетом. Нині інформація зберігається та накопичується у цифровій формі, що значно полегшує використання автоматичних методів обробки інформації.



Об'єм збережених даних у світі

Порівняйте скільки часу знадобиться, щоб знайти потрібне слово у рукописному конспекті чи на фото, і скільки часу потрібно щоб знайти те саме слово у текстовому файлі за допомогою функції пошуку? А якщо сторінок сто, мільйон?

Цифровий світ змінив підходи до зберігання, обробки та відтворення даних, зробивши ці операції набагато швидшими, а кількість інформації, що зберігається – майже нескінченою. Так за прогнозами до 2020 цифровий всесвіт досягне обсягу в 40 зеттабайт (це 40 з 21 нулем, що більше ніж діаметр нашої галактики у метрах).

Це величезний обсяг.

Інша відмінність у доступі до даних. Раніше всі данні зберігалися окремо, і щоб проаналізувати «вплив місячного сяйва на рейки», треба було окремо

отримувати дані щодо місячного сяйва у обсерваторіях, окремо дані щодо рейок у залізничників, а якщо ще в різних областях чи країна, то задача вирішувалась роками через різноманітну бюрократію.

Зараз більшість цифрових даних доступна через мережу Інтернет. Технологія відкритих даних набирає обертів і змушує відкривати доступ до величезних масивів даних.

Іноді дослідники просто всліпу аналізують інформацію у сховищах, і знаходять неймовірні закономірності. А якщо дослідник спрямовує свої зусилля на щось конкретне, то і результат матиме величезний вплив, хоч і дорого коштуватиме.

*В рамках системи оцінювання буде визначено рейтинг жителів Китаю, країни, чиє населення становить майже **1,3 мільярда людей**. Система буде визначати позицію громадянина, відстежуючи його соціальну поведінку: як він витрачає гроші, чи регулярно оплачує рахунки, навіть те, як він взаємодіє з іншими людьми. На цій публічній оцінці і буде засновано довіру до кожної окремої людини. Від рейтингу громадянина буде залежати, чи зможе він отримати роботу або іпотеку, а також в якій школі зможуть вчитися його діти.*

Те, що раніше здавалося лише фантастикою, тепер стає реальністю.

ТЕХНОЛОГІЇ BIG DATA

Сучасні інформаційні технології досягли того рівня, коли інформація у будь-якій сфері людської діяльності є величезною. Ця інформація має настільки великий обсяг, що для цього ввели спеціальний термін – Великі Дані. Проте великі дані – це не тільки великий обсяг інформації, але й методи її збору, обробки та аналізу, яка за своєю структурою є різнотипною та динамічною.

Інтернет, в якому ніколи нічого не пропадає і одного разу написане залишається назавжди, дозволив збирати величезні всеосяжні досьє на людей, компанії. При цьому значну частину необхідних відомостей вони публікують в Інтернет самі, добровільно: на сайтах, в блогах, соціальних мережах. Всі ці відомості в сукупності отримали назву Великі Дані. Знання Великих Даних дозволяє встановити, як поводиться людина в тій чи іншій ситуації, що для неї важливо, на що реагує сильніше за все. Це працює і для окремих людей, і для груп самого різного розміру – від декількох десятків до тисяч чоловік. Володіння Великими даними відкриває дорогу до прихованого управління поведінкою.

Сфера Великих Даних характеризується такими ознаками:

Обсяг – накопичена база даних, що містить великий обсяг інформації, який важко або неможливо обробити старими методами за прийнятний час.

Швидкість – вказує як на зростаючу швидкість накопичення даних (90% інформації було зібрано за останні 2 роки), так і на швидкість обробки даних, до обробки даних в реальному часі.

Різноманіття – можливість одночасної обробки структурованої і неструктурованої інформації. О найчастіше асоціюється з великим даними – це відео, аудіо файли, текст, дані з соціальних мереж, на сьогоднішній день вони складають 80% інформації. Проте вона потребує додаткової обробки та аналізу

Достовірність – чи можна вірити таким даним, чи правдива чи ні. Наприклад, дані, що генеруються ботами чи тролями у соціальних мережах.

Цінність накопиченої інформації. Досить складна ознака, адже ніколи не можна бути впевненим, чи зібрана інформація не може бути використана для якогось додаткового аналізу.

Фактично великі дані – це отримання якісно нових знань за рахунок комплексного аналізу усієї інформації у єдиному аналітичному сховищі.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВЕЛИКІ ДАНІ

Соціальні мережі є одним з найбільших інформаційних джерел світу. Оскільки соціальні мережі являють собою великий потік різнотипної інформації, необхідно застосовувати технології великих даних для їх збирання, структурування та обробки. Соціальні мережі – величезна база, яка складається з приватних та публічних повідомлень, інформації про користувачів, коментарів людей на те чи інше повідомлення тощо.

Великі дані та їх обробка

Чисельність користувачів найпопулярнішої соціальної мережі у світі Facebook сягає понад 2 мільярди осіб. Щоденно користувачі Facebook роблять

більш ніж 5 млрд публікацій, що є чудовим джерелом для дослідження населення будь-якої країни, базою для відстеження реакції людей на події.

Аналітична обробка великих даних дає змогу накопичувати знання, виявляти закономірності і виробляти оптимальні методи.

Після терористичного акту на Бостонському марафоні у 2013 році в США великі набори повідомлень, знімків і відеозаписів із соціальних мереж класифіковано та проаналізовано з допомогою високопродуктивних систем, що допомогло виявити організаторів теракту.

ДЖЕРЕЛА ДЛЯ ВЕЛИКИХ ДАНИХ

Джерела для подальшої обробки можуть найрізноманітніші. Більшість з них описані у міфі 3.

АНАЛІЗ ДАНИХ

Психологічний профіль людини будується на основі :

1. Аватар, статус, особисті дані
2. Список друзів.
3. Лента новин, пости, репости
4. Частота розміщення матеріалів
5. Фотографії, музика, відео
6. Участь у групах, громадах
7. Ведення власних тем, в тому числі професійних

На основі такої зібраної інформації можна визначити такі особливості людини:

1. Психологічний портрет, психотип, характер, відкритість
2. Цінності, моральні установки, рівень культури та виховання, сприйняття світу, мотивація, життєві пріоритети
3. Хобі, захоплення та інтереси, ритм життя,
4. Емоційний стан, настрій, рівень агресії, конфліктність
5. Громадське життя, громадянська позиція, політичні погляди
6. Професійні навики, досягнення
7. Репутація
8. Коло спілкування, місце у спільноті, кластери (учасник, вузол чи посередник)

НЕ ТІЛЬКИ АНАЛІЗ, АЛЕ Й ПРОГНОЗУВАННЯ

Важливим аспектом технології великих даних є можливість прогнозування подальших тенденцій на основі аналізу попередньо зібраних

даних. Це як прогноз погоди, тільки для різноманітних спільнот, або конкретної людини. Спрогнозувати, що люди будуть купувати в наступному сезоні, або за кого будуть голосувати на наступних виборах? Запросто! Великі дані допоможуть, і навіть врахують майбутні інформаційні впливи та події, що можуть трапитись. Звичайно, як і випадку з прогнозом погоди, тут є багато неточностей та невизначеностей, проте кожного дня користувачі всього світу перед виходом з дому цікавляться прогнозом погоди.

І якщо вплинути на погоду сучасними засобами людству ще не дуже вдається, то вплинути на громадську думку, виходить дуже добре. Прикладами можуть бути вибори в США, Brexit та агресія Росії проти України.

ПРОТИДІЯ

Не розміщуйте інформацію про себе, про свої уподобання, дозвілля тощо у соціальних чи будь-яких інших мережах.

Поводьтеся непередбачувано – відсутність типового профілю поведінки, дозволяє обійти сучасні системи аналізу поведінки та прогнозування реакцій.

Будьте готові до того, що інформація про ваші особливості доступна різним особам, вивчайте свої слабкі місця, вчиться змінювати свої реакції на соціальні подразники – робіть собі інформаційну вакцинацію.

МІФ 5. В СОЦМЕРЕЖАХ (ЗМІ) КАЖУТЬ ПРАВДУ

Люди, які вірять в цей міф, люблять дивитись телевізор, гортати соціальні мережі і вважають абсолютно всі повідомлення достовірними. «В новинах передали», «в інтернеті написали» – цього достатньо аби будь-яку нісенітницю вважати правдою.

Міф 5. В соцмережах (ЗМІ)кажуть правду

Насправді

Фейкові новини, дезінформації, ланцюгові передруки інформації без перевірки джерел, коментарі та емоції під виглядом новин – звична практика українських ЗМІ та соціальних мереж. Часто передруковуються новини з інших ЗМІ, блогів і, навіть, постів у соцмережах без належної перевірки того, що було подано, так і авторитетності цих новин. Джерелом може бути невеличке партійне видання (Washington Free Beacon) або таблоїд (Daily Express) або взагалі блог нікому не відомого експерта. Через такі медіа-практики в інформаційному просторі України поширюється ворожа пропаганда.

Новини в Україні часто виглядають як трансляція відомої української приказки про дядька з Києва і бузину на городі. Стандартний репортаж кореспондента у телевізійному випуску новин в Україні. Повідомлення №1 «На городі бузина». Повідомлення №2. «У Києві дядько». Уважний глядач навряд чи вловить зв'язок між цими двома повідомленнями, але якщо вони подаються одне за другим, отже, можливо і пов'язані? Про зв'язок, звичайно, сповістить кореспондент у повідомленні №3. Це висновок і він звучить так: «За те я тебе полюбив, що на небі місяць». Що за нісенітниця, мав би сказати наш з вами уважний глядач. Але, на жаль, враховуючи психологічні особливості уважного глядача, він у захваті чи в паніці сприйме набір нісенітниць, як аксіому, що не потребує доведення.

Якщо ми без упередження ще раз прослухаємо новини, то виявиться, що перше і друге повідомлення – чиста правда. Бузина може рости на городі, правда, в реаліях Вінницької області город з бузиною наче вже і не город, а дядько – може жити в Києві. Ця основна частина готує нас до сприйняття і передачі далі висновку, який дещо нераціональний, але вірогідність перших двох повідомлень дозволяє повірити у зв'язок між Місяцем і особливими неповторними якостями коханої, які спричинили спалах почуттів до неї.

За цієї схемою будуються повідомлення про внутрішню і зовнішню політику, місцеві новини, репортажі з АТО, життєві історії в соціальних мережах.

Пенсінерка-переселенка втратила дім і три роки бідує (докладно описуються бідування жінки). Пенсіонерці хочеться з кимось поговорити і вона постійно приходить у волонтерську організацію (опис волонтерської групи, яка допомагає переселенцям, але ресурси невеликі). Наче нейтральний допис, читачі налаштувались на співчуття до пенсіонерки, підтримку волонтерської організації, і тут висновок – ненавиджу українську владу, це вона в усьому винна.

Логічно було б звинуватити в бідах пенсіонерки тих, хто зруйнував її дім, почав збройний конфлікт, анексував Крим, однак стрілки вміло переведені на

українську владу. Посіяти недовіру до української влади – одне з завдань інформаційної війни.

Інше завдання – наповнити український простір подіями, історіями і культурними досягненнями Росії, особливо періоду двадцятого століття. Фальсифікації поширюються щодо українських визвольних змагань, подій другої світової війни, побутового життя в СРСР. Звичайно, менше з вуст політиків, більше – на екранах телевізорів, в сюжетах серіалів, безконечних розповідях про особисте життя радянських акторів – все це покликане створити в людей ілюзію значимості Росії та СРСР, особливих досягнень літератури і культури, які там наче б то там були.

ФЕЙКОВІ НОВИНИ

Google і Facebook заявили, що збираються найняти велику кількість людей, які перевірятимуть контент, стежитимуть за дотриманням умов надання послуг і усуватимуть фальшиву та протизаконну інформацію зі своїх платформ. Хотілося б подивитись, як вони це робитимуть

Крейґ Сілверман з видання Buzzfeed.

Фейкові новини – це повністю або частково вигадана інформація про суспільні події, справжніх людей, або про речі, явища, яка подається під виглядом справжніх. Використовуються як зброя в інформаційній війні .

Засоби підтвердження фейкових новин:

- Фотофейк – змонтоване фото; фото, в якому не правильно вказані місце, дата, події;
- Відеофейк – аналогічне фотофейку, але тут набагато частіше зустрічаються змонтовані або перемонтовані відео.
- Фейкові свідчення очевидців – використовуються посилання на відомих людей, які навіть не знають про подібні новини; підставні свідки; свідки, які навіть не були присутні у подіях, що описуються.
- Фейкові експерти – основна ознака - дуже проста або дуже захаращення термінами мова, а також велика кількість регалій. Та якщо ввести прізвище експерта в пошукову система – вона покаже його мало значимість та відсутність відповідної кваліфікації.
- Фейкові повідомлення від імені західних ЗМІ – базуються на тому, що переважна кількість користувачів фейкових новин не знають жодної іноземної мови, зокрема англійської, і мають великий пієтет до «західних ЗМІ», не розрізняючи авторитетні видання та «жовту» пресу.

Фейки можуть бути позитивні, нейтральні та негативні.

Позитивні фейки

Фейки не тільки поширюють негативну інформацію, існують так звані позитивні фейки, більшість яких спрямована на розповсюдження позитивних новин про здобутки України. Одним з найбільш відомих позитивних фейків є повідомлення про визнання гімну України найкращим в світі, поширене в 2013. Ось його текст.

Центр світової спадщини ЮНЕСКО визнав гімн України найкращим в світі. Про це повідомляє Інтерфакс-Україна з посиланням на Центр новин ООН. До рейтингу увійшли національні гімни 193 країн. Гімн України здобув перше місце в загальному рейтингу. При цьому, до уваги брались 4 показники, по двох з них українських гімн отримав найвищий бал – милозвучність, гармонійне поєднання музичної та текстуальної частин. Високий бал також давали за оригінальність музичного рішення та цілісність твору.

Інформацію про перемогу українського гімну у світовому конкурсі ЮНЕСКО передрукували, не перевіривши, журналісти близько ста видань, серед них «Газета.ua», «Экономические Известия», «Бизнес.ua», «Голос.ua», «Ура-Інформ», «Свідомо».

Приклад позитивного фейку розповсюдженого серед ЗМІ

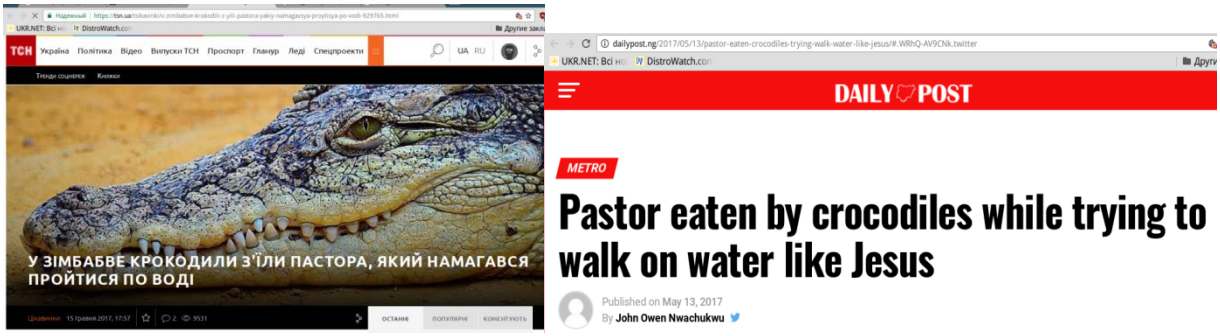
Чи шкодять позитивні фейки? Можливо, варто їх творити все більше і більше, і саме в цьому суть інформаційної політики? На жаль, ні. Позитивний фейк, потішивши людину, неминуче закінчиться негативними емоціями і розчаруванням, і тоді провокуватиме недовіру до українського. Остання ланка в ланцюжку позитивних фейків – теза про меншовартість українців, які, начебто, не мають реальних досягнень і вимушені їх вигадувати.

Внаслідок цього навіть справжні позитивні новини викличуть недовіру і загальне занепокоєння, чи не прикривають ними негатив.

Нейтральні фейки

Однією з найвідоміших фейкових новин є історія про підтвердження американськими вченими існування русалок, яку передрукували ряд провідних українських ЗМІ у вересні 2013 року. Це ще один приклад ланцюгових передруків без перевірки, які практикують ЗМІ в Україні. Особливістю цієї новини є те, що вона є передруком з американського ЗМІ, яке славиться своїми вигадками, фактично це газета фейків, «**Weekly World News**». Шанувальники фільму «Люди в чорному» знають цю газету – саме з неї герої фільму отримували правдиві новини про прибульців. В 2013 році такими новинами «годували» українців і стверджували, що це правда.

Не менш гучної стала розповідь про пастора, який гуляв по воді, але його з'їли крокодили.



Нейтральний фейк про пастора, якого з'їли крокодили, коли він гуляв по воді

Ця фейкова новина фактично показала, як легко створити новину, яку поширять величезна кількість ЗМІ, і не тільки українських, без перевірки. Якби хоч хтось звернув увагу на першоджерело – невелику сатиричну газету, то про цю історію навіть ніхто б і не знав.

Новини «про русалок та крокодилів» створюють інформаційний шум, в якому людина поступово вчиться сприймати будь-яку вигадку за правду. Не вміючи і не бажаючи включати внутрішнього критика.

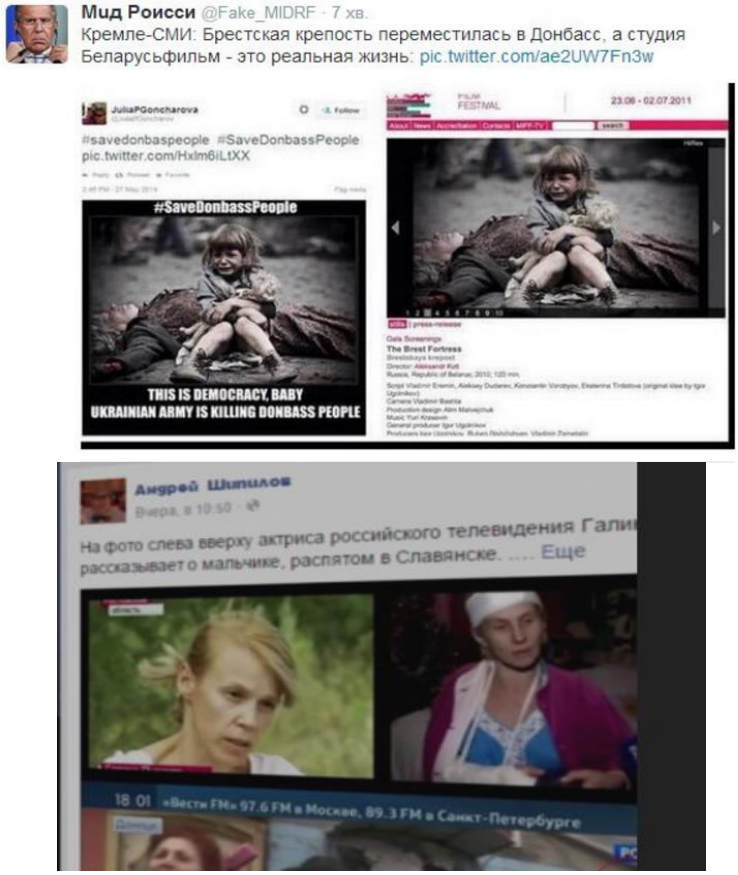
Будь-які нові знання необхідно аналізувати – не важливо фейкові вони чи ні – щодо їх відносної правдивості. Звичка та вміння до аналізу інформації набувається досить складно, і потребує спеціального навчання, зазвичай починаючі з дитинства, з якісної освіти. Проте сучасні освітні заклади часто не вчать аналізувати, тому ці навички треба здобувати самостійно.

Негативні фейки

Найчастіше фейки мають негативне забарвлення, і/або провокують негативні емоції.

Міф 5. В соцмережах (ЗМІ)кажуть правду

Справжній розквіт фейкових новин припав на 2014-2015 роки. Фото біженців з Косова подавалось як фото переселенців з Донбасу, встановлена в центрі Вінниці шибениця лякала російських родичів, фото російських військових в засніженому окопі називалось українським, порнозірка стала моделлю для історії замученої укропами медсестри, а численні «два раби», «розіп'яті хлопчики» та снігурі морочили голову російським громадянам і роз'єднували родини.



Кілька прикладів негативних шейків

Влітку 2014 року з далекої Росії на Вінниччину вирушив на батьківщину літній чоловік. Втім, він не доїхав навіть до кордону. Злякався. Зателефонував родичам і повідомив, що «не їду, бо ви там дітей їсте.» Історія зовсім не смішна, бо в різних варіаціях її розповідають про всій Вінницький області, якими б абсурдними не здавались фейкові новини, люди вірили їм більше, ніж своїм родичам.

Окремий вид фейкових новин – дезінформація щодо дій української влади. Особливо багато їх стосується бюджету, податків, субсидій, служби в армії. Піл час прийняття змін до законодавства, розповсюджуються чутки про їх негативний вплив на життя людей, наприклад, змусять повертати субсидії, значно збільшать податки, чоловікам старше 45 років заборонять виїзд за кордон, а поховати небіжчика можна буде тільки після рішення суду. Кожна

така новина розрахована на провокування паніки серед якнайбільшої кількості людей, адже субсидії, похорони, податки та армія – теми, які так чи інакше стосуються ледь не кожної родини в Україні. Варто звернути увагу на час поширення чуток, наприклад, чутки про заборону виїзду чоловіків за кордон розповсюджувались напередодні зимових свят, коли люди традиційно налаштовані на гарний настрій і мають позитивні плани.

Часто фейкові новини поєднуються з розповсюдження чуток в реалі. Розглянемо приклад подій у Вінниці 7-8 травня 2014 року. В ці дні у місті розповсюджувались чутки про можливу появу «зелених чоловічків» і провокації. Паніка досягла таких масштабів, що переносились заплановані заходи, батьки забирали дітей з садочків і шкіл, люди масово знімали гроші з банкоматів. Чутки розповсюджувались через конкретних людей і через спеціально створені сторінки у ФБ. Кілька таких сторінок подавались, як створені грузинами (розрахунок на те, що Грузія союзниця Україні в боротьбі проти Росії). Також варто врахувати, що профілі цих сторінок були заповнені грузинською мовою і зрозуміти про що і про кого мова було важко. Але «дружні грузини» одночасно перепощували новини про появу російських військових, то в Умані, то ще десь ближче до Вінниці. На жаль, вінницькі активісти не одразу зрозуміли, що проти міста ведеться спеціальна операція, аби посилити паніку і страх. А коли зрозуміли, то почали протидіяти. Найбільш ефективною виявилась гумористична кампанія «Вінниця, узбагойся», та «гарячі новини» від волонтерки і громадської діячки Лариси Полулях, яка оголосила, що тільки на її сторінці буде подаватись найправдивіша інформація, і ледь не кожну годину постила допис про «чеченців і кенгуру в салатових трусах», які атакують фонтан у Вінниці. Спільними зусиллями влади і громадських активістів вдалося погасити паніку.

Наслідки фейків

Чому негативні фейки такі мають такий ефективний вплив і чому боротися з ними так складно.

У фейків є дві складові впливу.

Безпосередній, у момент розповсюдження, який провокує паніку, бажання забрати всі гроші з банкомату, чи подзвонити всім родичам і знайомим і повторити цю новину не менше чотирьох разів різним людям. (До речі, останнє – психологічна особливість боротьби зі стресом, яку використовують, в тому числі для різноманітних терапій). Всі ці дії лише посилюють паніку, розповсюджуючи її серед все більшої кількості людей та спільнот.

Особливо, коли розповсюджувачем стає якась соціально значима особа (соціальний посередник або вузол). Таким людям необхідно уважніше

ставитись до розповсюдження новин, перевіряти походження та запитувати себе «навіщо це потрібно, які наслідки» .

Довготривалий вплив є ще більш небезпечним. Адже, для того щоб перебити негативну новину, треба отримати не менше трьох різних спростувань.

Розповсюджуючи негативні фейки, агресору навіть не треба особливо щось придумувати чи формувати схожі на правду повідомлення. Навіть, якщо ці новини будуть спростовані, вони все одно будуть формувати посилення тривожності. І чим більше фейкових новин, тим більшим буде почуття тривожності, недовіри та внутрішньої напруженості у суспільстві, навіть, якщо ні слова правди у цих фейках не має.

Винаходом «гібридної» війни, яку ще остерігаються назвати Третьою світовою, стала фейкова бомба. Це також зброя масового ураження. Вона залишає незаторкнутими будівлі, інфраструктуру й навіть людські тіла. Вражає, натомість, лише людську душу. Найголовніша сила глибокого ураження у фейковій бомбі – це Недовіра. Її жертви – розгублені люди, які неспроможні відрізнити правду від брехні. Її символи – дискредитація українського Майдану, Брекзіт і підірвані виборчі системи західних демократій.

Мирослав Маринович

Різні фейки для різних людей

Внаслідок розвитку інформаційних технологій багато людей читають новини через Інтернет, вважаючи, що саме там можна отримати незаангажовану, незалежну від влади (опозиції, агресора потрібне підкреслити) інформацію. Проте вони забувають, про те, що розвиток аналізу даних про самого користувача (читай міфи 2, 3) дозволяє формувати саме ті новини, які будуть мати вплив на цього користувача незалежно від його уподобань.

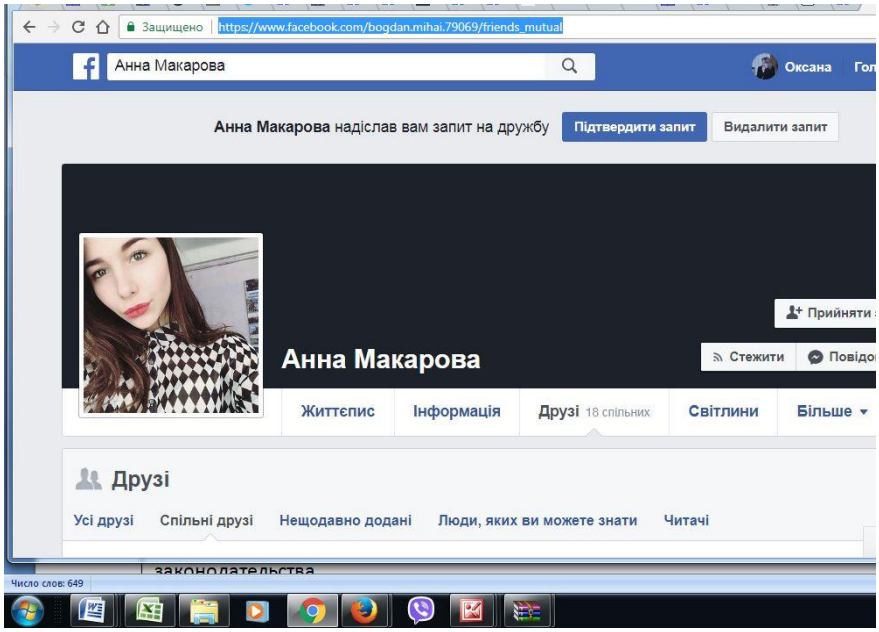
Так., це складно, і вимагає багатьох ресурсів, але згадайте таке. Після того як ви ввели в пошук «який смартфон купити» або просто «смартфон», вам обов’язково протягом деякого часу буде відображатися контекстна реклама зі смартфонами.

Аналогічно відбуваєтьсь зі стрічкою новини. Під різники аккаунтами, можна побачити різні стрічки новин залежно від того, що зацікавило раніше. Якщо система бачить, що ви з України, новини будуть одні, а якщо з Німеччини – інші.

БОТИ, ТРОЛІ ТА ІНША НЕЧИСТЬ

Хто такі боти

Віртуали або боти – це профілі і сторінки в соціальних мережах, які створені неіснуючими в реальності людьми. Одна людина може вести кілька сторінок. Ботами таких персонажів називають через аналогію з комп'ютерними програмами-роботами, які використовуються для поширення та моніторингу інформації в Інтернет. Багато користувачів соціальних мереж нехтують правилами безпеки і не перевіряють профілі тих, кого додають у друзі. Навіть виявивши сторінку бота, люди вважають, що тут нема нічого страшного, це «продажники», а сторінка створена, аби просувати товари чи послуги.



Сторінка бота. В посиланні можна прочитати – Богдан Мігай. На сторінці – Анна Макарова.

Найбільша небезпека ботів у тому, що їх наміри невідомі. Можливо, вам збираються запропонувати купити косметику, а можливо – додались з метою поскаржитись на вашу сторінку і заблокувати її. Або хочуть ввійти в довіру і видурити у вас гроші чи майно. Або за ботами ховається певна політична сила, якій потрібен ваш голос на виборах і вона непомітно, день за днем, впливатиме на вашу думку. Або гарна молода дівчина насправді хоче витягти інформацію від українських військових. Варіантів – безліч. Додаючи ботів у друзі ви не тільки самі наражаєтесь на небезпеку, але й легітимізуєте бота в своїй спільноті. Фактично, приводите в родину шахраїв.

Українські користувачі Facebook та інших соціальних мереж не раз фіксували організованих російських віртуалів-ботів, які діють проти України. Зокрема, цілеспрямовано працюють на блокування сторінок відомих українських користувачів соцмереж, підбурюють на виступи проти влади.

На початку 2016 року видання «Укрінформ» виявило систему ботів у соцмережах, які поширюють в Інтернет заклики до насилля до української влади та заклики виходити на «Третій Майдан».

Журналістка Укрінформу Лана Самохвалова розповіла про групу у ФБ «Всі на Майдан». Створив групу громадський активіст Степан Мазура. В групі було багато антиукраїнської інформації. Фейкові повідомлення поєднувались з реальними критичними матеріалами українських ЗМІ, маніпулятивні опитування на тему «усунути Порошенко» із прогнозами фейкових експертів про повний неуспіх або навіть розпад України. Крім поширення аналітики, активно спілкувався з читачами у коментарях. Когось ігнорував, з кимось спілкувався в стилі «старі друзі», ветеранів АТО називав «цвітом нації» і одночасно протиставляв їх «продажній владі», комусь робив компліменти, обіцяючи поставити фото в своїй групі, тобто підвищити в соціальному ранзі.

В результаті проведеного розслідування з'ясувалось, що справжнє ім'я Степана Мазури – Сергій Жук. У сепаратиських загонах він має псевдо «Москва». Але найцікавіше, що доступ до профілів Степана Мазури у соцмережах здійснюється з використанням IP-адрес, що належить Інтернет-провайдеру PJSC Rostelecom, РФ (м. Москва). Степан Мазура виявився одним з армії найнятих російською владою блогерів, які працюють проти України. Ймовірно, що псевдонім приховує групу фахівців з інформаційної війни.

Тролінг в соціальних мережах

Одним із найпоширеніших у соціальних мережах різновидів інформаційно-психологічних операцій є тролінг (англ. trolling – «виспівувати»), що застосовується для формування суспільної думки з актуальних питань та активного обговорення другорядних подій.

Інформаційні операції максимально ефективні тільки тоді, коли людська свідомість знаходиться у нестійкому стані, знаючи особливості людини, тролі створюють спеціально підготовлену інформацію з елементами маніпулятивного впливу, які дозволяють перевести людину у нестійкий стан.

Інтернетний троль – це людина, яка розміщує брутальні або провокаційні повідомлення, наприклад, у дискусійних форумах, групах, під дописами користувачів і перешкоджає обговоренню або ображає його учасників.

В соціальних Інтернет-сервісах тролі як засоби агресивного впливу поділяються на:

- **природні**, користувачі, які, як правило, спеціально тролінгом не займаються, просто в них характер такий;

Трагічна історія американської дівчинки Меган Майерс, яка в 2006 році наклала на себе руки через Інтернет цькування. 15-річна дівчина познайомилась в Інтернеті з хлопцем Джошем, який зізнався у коханні, майже місяць тривало віртуальне романтичне спілкування, а потім Джош почав грубо поводитись з Меган, ображав її і врешті-решт, написав, що світ був би набагато кращим без неї. Через двадцять хвилин після отримання цього повідомлення Меган наклала на себе руки. Пізніше з'ясувалось, що Джоша ніколи не існувало в реальності, його сторінку в соціальних мережах створила мама колишньої подружки Меган, щоб з'ясувати, що Меган пише про її доньку. Загалом, сторінку Джоша вели три людини. Мабуть, їх відчуття безкарності були настільки сильним, що вони, не задумуючись, ображали 15-річну Меган і писали їй всі ті речі, які ніколи не наважились би висловити в реальності. Варто зазначити, що 49-річна Лора Дрю, ініціаторка цькування, була засуджена, але вирок скасували, бо, фактично, не існувало законів, які вона порушила, окрім угоди користувача соцмереж.

абсолютно кожна людина може стати об'єктом для цькування з боку тролів, треба дуже уважно ставитись до того, з ким спілкуєшся, і як це спілкування впливає.

- **професійні** – особи, які залишають коментарі в соціальних мережах за завданням урядових структур. Такі тролі коментують за гроші для пропаганди або розміщення політичної реклами під новинами на форумах, блогах або на інших соціальних ресурсах в мережі. З описів роботи російських «тролів в Ольгіно» (термін виник від місця, в якому базуються одна з груп інформаційного впливу в Санкт-Петерурзі) дізнаємось, що їх ефективність вимірюється об'ємом написаного тексту, а також вмінням створити діалог і просувати свою думку. Чим більше коментарів отримає троль на своє повідомлення, тим успішнішою вважатиме свою роботу. Не має значення, чи він проплачений спецслужбами або піар-агенствами, чи волонтер, запрограмований російськими ЗМІ .

Основна мета Росії в інформаційній війні – не стільки просування своєї точки зору, скільки деморалізація і дистресизація населення, що наносить шкоду не лише психічному, але й фізичному здоров'ю.

Ольга Малишева

Фейк і пропаганда: як армія кремлеботів прикидалася американцями

Карикатура на тему кремлеботів

- **ботів** – програма, яка імітує діяльність людини через користувацькі інтерфейси, і як і професійний троль розповсюджує спеціально підготовлені повідомлення на різну тематику.

Ознаки тролів в соціальних мережах

- негативна тональність повідомлень;
- емоційність повідомлень;
- сумнівність наведених фактів;
- сенсаційність повідомлення;
- повідомлення у великій кількості від одного автора;
- дублікати повідомлень на різних сайтах та постах.

Завдання тролів

- виведення людини з рівноваги і, як наслідок, сприймання нею потрібної тролю інформації, в решті до зміни картини світу;
- провокування агресії у людини і, як наслідок, втрата нею авторитету у суспільстві;
- компрометація ресурсу (мережевої спільноти) за рахунок нагнітання агресії у самій спільноті, що призводить до зменшення авторитету спільноти та, відповідно, дискредитація ідей, що вона відстоює;
- формування думки, що оточення людини, вважає так само, як і троль, а отже людина починає сумніватись у власній картині світу;
- формування думки, що всі навколо думають, як троль, а отже, підміна думки суспільства;
- блокування ресурсу (мережевої спільноти) за рахунок використання нецензурної лексики та мови ненависті тощо;
- компрометація ресурсу (мережевої спільноти) за рахунок використання перекручених фактів, фейків та безглуздих висловлювань;

- відволікання уваги від теми інформаційного ресурсу, і засмічення його інформаційним шумом з метою дискредитації ресурсу.

Компанія Facebook оголосила, що компанія «Інтернет-дослідницьке агентство» (воно ж «Агенство інтернет-дослідження», або «Фабрика тролей»), яка базується в Санкт-Петербурзі, витратила близько 100 тисяч доларів на рекламу в соцмережі. 470 ботів написало 80 тисяч постів, які стосувалися теми американських виборів. «Фейки» також розмістили близько 120 тисяч публікацій в Instagram. Соцмережа Twitter виявила близько 50 тисяч кремлеботів.

https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/

В результаті розслідувань державними органами США зафіксовано втручання Росії у хід виборів Президента США у 2016 році. Багато з технологій, які використовувались у США російськими «фабриками тролів», ймовірно працюють і в Україні. Серед них – намагання будь-якими засобами поляризувати суспільство, нав’язавши йому дискусію щодо певних питань, національності, імміграції, ЛГБТ. Як каже один з героїв американського серіалу «Homeland», роздмухування локальних незгод до велетенського конфлікту – улюблений метод росіян.

Кремлеботи з «Серця Техасу» організували мітинг в Х'юстоні «Зупинити ісламізацію Техасу». У відповідь в тому ж місці і в той же час, група «Об'єднані мусульмани Америки» організували мітинг «Збереження ісламського знання» (справа російських тролів). У підсумку, десятки людей, які прийшли на мітинг, прихопивши з собою рушниці, зіткнулися з натовпом протестувальників американських мусульман. Поліція швидко відреагувала і тримала протестуючих на відстані один від одного. Пізніше деякі спантеличені учасники поскаржилися, що ніхто з організаторів групи «Серця Техасу» на заході помічений не був.

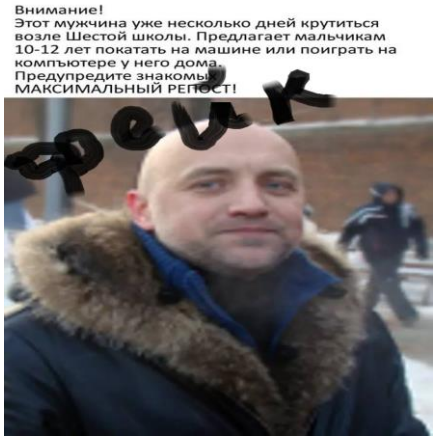
Компанія Facebook повідомила, що близько 130 мітингів були організовані за допомогою 13 російських груп. Передплатників групи найчастіше залучали дискусійними в американському суспільстві темами: національність, зброя, імміграція, ЛГБТ.

Одна з тих речей, через які я найбільше жалкую, це те, що ми були повільними у виявленні російських інформаційних операцій у 2016 році.

Марк Цукерберг, засновник ФБ

Міф 5. В соцмережах (ЗМІ)кажуть правду

У Вінниці в 2018 шукали педофілів. В ФБ з'являється профіль вінничанки, кілька фото, сімейна ідилія, діти, відпочинок на природі, вказано номер школи, в якій навчалась. Правда, ніхто з випускників цієї школі поки що не згадав її, але всяке буває, вийшла заміж, зовнішність з роками теж змінюється. В кінці березня 2018 року вінничанка викладає у профілі фото чоловіка з підписом «цей чоловік вже кілька днів крутиться біля шостої школи, пропонує хлопчикам 10-12 років покататись на машині чи пограти на комп'ютері в нього вдома.» Обурені вінничани почали масово перемощувати фото. За кілька тижнів – 70 тисяч перепостів з панічною інформацією для батьків, тисячі коментарів. І між ними – самотні повідомлення «агов, на фото російський письменник Захар Прилепін, відомий своєю підтримкою сепаратистів на Сході України». Сто поширювачам допису про «педофіла біля школи» були написані коментарів про те, що допис – фейк. Відгукнулись 5, четверо подякували, видалили, одна особа – написала, що їй байдуже, хто на фото, головне – попередити батьків про небезпеку для дітей. Подібна кампанія у США закінчилась збройним нападом на одну з піццерій, «поінформований соціальними мережами» громадянин США зчинив стрілянину в приміщенні, бо вважав, що там незаконну утримують дітей.



Скрін сторінки з повідомленням про чоловіка біля школи

Толеруючи фейки і ботів українські громадяни наражаються на серйозний ризик, хто зна' чиє фото оберуть для страшилки про педофілів наступного разу, і на які дії зважаться підбурені батьки.

ПРОТИДІЯ

Застосовуйте «презумпцію брехливості»: привчіть себе будь-які новини, чи зі ЗМІ, чи з соцмереж вважати брехнею і не реагувати на них. Якщо новина для вас важлива – витратить час на перевірку, якщо вона вас не стосується – ніяк не реагуйте, не коментуйте, не перепощуйте.

- Перевірте фото – чи на ньому справді ті люди, про яких пишуть в новині, в Google можна відшукати подібні фото.
- Перевірте посилання на джерело – якщо мова про новий закон/постанову/указ, знайдіть його на сайті Верховної ради/Президента/Кабінету міністрів і прочитайте.
- Перевірте експертів – чи вони справді існують, в Google можна знайти посилання на ще якісь експертні коментарі, окрім цього.
- Перевірте джерело, яке створило цю новину, чи не має сторінка ознаки ботів чи фейків, поцікавтесь у спільних друзів, чи знає хтось цю людину особисто, перегляньте попередні поширені на сторінці повідомлення – чи є там щось, крім «шок-масимальний перепост»

Не довіряйте сенсаційним повідомленням («Шок», «Максимальний перепост», «Ця новина вразила Інтернет», «Розкажи друзям»), не зважаючи, який зміст, позитивний чи негативний, вони несуть. Перш ніж реагувати, постити, радіти чи осуджувати, перевірте цю інформацію та її джерело.

Привчіть себе не реагувати на провокативні повідомлення, особливо, якщо вони викликають у вас емоції чи агресію.

Не ведіть суперечки з тролями – це марна трата часу, припиняйте спілкування одразу, якщо конче потрібно вступити в полеміку – не піддавайтесь емоціям, апелюйте до фактів.

Якщо ви побачили або виявили фейк, інформуйте про це друзів і знайомих. Давайте спростування, але тільки із залученням фактів та доказів.

Не додавайте у друзі в соцмережах людей, яких ви не знаєте особисто!

Вивчайте іноземні мови. Користуйтесь гугл-перекладачем. Це допоможе перевірити новини, в якій посилаються на заяви іноземних діячів, повідомлення іноземних ЗМІ.

Пишіть своє. Замість перепостів створюйте власні новини: розкажіть цікаві історії з життя ваших предків, поділіться враженнями про фільми чи книжки, опишіть власний досвід громадської активності.

Уникайте висновків та узагальнень, вони провокують конфлікт, розповідайте історії і діліться емоціями – це об’єднує і допомагає знайти порозуміння.

МІФ 6. НА МЕНЕ ВПЛИНУТИ (ОБДУРИТИ) НЕ МОЖЛИВО

Шанувальники цього міфу вважають, що маніпулювати можна певним типом людей, тими, хто не впевнений, слабохарактерний чи малоосвічений. Вірять, що є люди, які мають вроджений дар відрізняти брехню від правди, і на них вплинути неможливо.

Насправді

Більшість методів впливу на поведінку людей використовують неусвідомлені процеси в мозку людини. Вплив відбувається миттєво, і люди не помічають його навіть при багаторазових повтореннях, а свої реакції і дії вважають свідомим вибором.

МАНІПУЛЯЦІЯ СВІДОМІСТЮ

Робота аналітичного мислення – це те, проти чого працюють російські медіа, бо їх мета змусити людей не аналізувати інформацію взагалі

Наталія Зубар,
голова правління Інформаційного центру Майдан Моніторинг.

У нашому світі все підкоряється закону збереження енергії. Тому, якщо людина у власному житті не використовує волю, свідомість, увагу, то всім цим скористається хтось інший.

Мудрість з Інтернет

Маніпуляція свідомістю є у всіх сферах суспільного життя. Різноманітні цінності пропагуються через пріоритети виховання, через освіту, мистецтво та літературу. У політичній сфері пропагуються іміджі і привабливі, з точки зору маніпулятора, носії політичних ідей за допомогою, політичної реклами та засобів масової інформації.

У широкому сенсі маніпуляція – це певний вплив на свідомість і поведінку людини або соціальних груп.

У більш вузькому сенсі «маніпуляція свідомістю» – це свідомий та цілеспрямований вплив на людину з метою змін у думках, оцінках, поведінці і переконаннях, вигідних маніпулятору.

ЯК НА НАС ВПЛИВАЮТЬ – ВІДЗЕРКАЛЕННЯ

Маніпуляції? Прихований вплив? Люди чують ці слова і уявляють ворожку з лялькою вуду, віск, шепотіння, весь той магічний набір, який на Поділлі називають словом «пороблено».

Насправді вплив на людину відбувається при кожній комунікації. Зустріли знайомих, прийшли на роботу, на каву, в гості – всюди при контактах людей відбувається миттєва взаємодія ще до того, як почалась розмова. Ззовні це виглядає як ледь помітне скорочення м’язів і називається **віддзеркалення**. Люди несвідомо зчитують позу одне одного, емоції і відображають емоційний стан інших. Суть віддзеркалення в тому, що людина з впевненою поведінкою,

гарною поставою і позитивними емоціями має більший вплив при спілкуванні, її емоції **дзеркаляться** іншими. Несвідомо ця людина отримує в спільноті вищий статус, її повідомлення викликають довіру, інші члени спільноти прагнуть більше спілкуватись з нею. Щось в мозку наче говорить їм: «вір цій людині, вона допоможе вбити мамонта, захистити від ворогів і вирішити твої проблеми».

Звичайно, наше виживання не залежить від вбивства мамонта. Чому ж тоді люди так прагнуть товариства спокійних і впевнених? Справа в тому, що абсолютно всі люди мають постійну неусвідомлену тривогу, рівень якої можна посилити або послабити.

При контактах з впевненими людьми тривога послаблюється, людина відчуває миттєве заспокоєння і почуває себе краще. Здається, шлях для впливу на людей простий – транслюй позитивні емоції, працюй над поставою і вчись бути розслабленим? Довгий шлях.

Диктатори і шахраї обирають легший і простіший спосіб – маніпулювати людиною, збити з пантелику. Як? Посилюючи базову тривожність людини. Можна транслювати погано розпізнавані емоції, лагідним голосом закликати вбити сусіда чи відволікати увагу різними жестами. Лякати страшилками і обіцяти порятунок. Якщо такий вплив триматиме 3-4 тижні, то тривожність почне підсилюватись сама по собі.

Для більшої ефективності можна застосувати традиційні диктаторські заходи – зробити так, аби результат дій людини не залежав від її зусиль. Скільки б ви не працювали, вам не дозволять жити краще на інших, які б здібності ви не мали – ви не зможете їх використати через соціальний стан, національність, чи родичів «врагів народу».

Геніальний український поет Василь Стус в ув’язненні монтував детальку до праски, день у день, одна і та ж робота. Рукопис книжки психотерапевта Віктора Франкла в перший день перебування у німецькому концтаборі викинули на сміття. В’язні концтаборів могли мати скільки завгодно позитивних якостей, але перебуваючи в умовах невизначеності і загрози життю важко зберігати спокійну впевненість.

Але ж у нас нема диктатури? Тобі треба посилювати тривожність загрозою – переконувати, що все погано, займатись підприємництвом нема жодного сенсу, поширювати спеціально підібрані фейки. Це змушує одних шукати втіху в алкоголі та побутовому насильстві, а інших – переконує в марності будь-яких спроб покращити своє життя. Надмірно стривожене суспільство стає легкою здобиччю для агресора, диктаторів та шахраїв.

Трансляція основних повідомлень, як вербальних, так і невербальних відбувається в прайм-тайм, коли телевізор не слухають, а дивляться, і дивляться уважно, приділяючи увагу не лише звуку, але й відеоряду. Сюжети ці ретельно підготовані: на передньому плані ведучий, – чоловік статусного вигляду, що перебуває в хорошій фізичній формі, з блискучими очима і впевненими манерами, вже відомий аудиторії не лише за іменем і виглядом, але й завдяки участі, в тій, чи іншій формі, в розважальних передачах. … аудиторія не лише прислухається до його слів, але й відслідковує і "віддзеркалює" міміку. Такій поведінці сприяє і так звана "драматична дикторська манера", мета якої – транслювати емоцію модуляціями і інтонуванням, як актор на сцені. …використовується неспівпадіння вербального змісту повідомлення і дикторської емоції: відверто жахлива історія може бути розказана сумно і навіть лірично, більш нейтральна – скорботно, така, що містить жорстку лексику на грані обсценної – лагідно чи грайливо.Якщо сюжет стосується "ворога", тон повідомлення буде, найімовірніше обережно-ворожим або й нейтральним, але з елементом відрази і вживанням елементів відповідної "відразливої" лексики. Якщо він стосується "жертви" – агресивним, зневажливим, з використанням відповідного нормативного гумору, саркастичним.ркастичним.

Ольга Малишева https://maidan.org.ua/2015/06/olha-malysheva-yak-vyhraty-informvijnu-chastyna-1-vijna-sotsialnyh-emotsij/

МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Людська цивілізація вдосконалила давню техніку віддзеркалення і створила науку – соціальну інженерію. Вона базується на тому, що саме людина є найслабкішою ланкою будь-якої системи. Саме тому, за умови, що технічно отримати якусь інформацію або змінити щось в системі досить важко, впливають **безпосередньо на людину**.

Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи не вчинили б з доброї волі. Бо хто, при здоровому глузді, озвучить по телефону пароль до онлайн-банкінгу, чи дозволить встановити підозрілу програму на власний комп'ютер? Чи оприлюднить в соціальних мережах інформацію про свій маршрут в зону бойових дій ? Вийде на мітинг в підтримку ідей, про які щойно дізнався?.

Маніпулятор часто застосовує заздалегідь розроблений сценарій, щоб спонукати жертву до дій, яких у звичайних обставинах вона не вдалася б. Атаці

передує збір інформації про жертву, її інтереси, оточення, уподобання та інформаційні меми , що на неї можуть вплинути.

Небезпекою таких методів маніпулювання та їх комбінацій є те, що на них піддаються всі люди.

МАНІПУЛЮВАННЮ ПІДДАЮТЬСЯ ВСІ. ВИНЯТКІВ НЕМАЄ.

Просто хтось є більш стійким, хтось – менш.

Значний ефект, що посилює можливість протистояти маніпулюванню є навчання методам і способам маніпуляції, проведення тренувань та виявлення мемів, на які людина може зреагувати.

Методи маніпулювання

Для впливу на жертву маніпулятор застосовує досить не велику кількість методів, що базуються на психологічних особливостях людини.

- ***провокація*** – виведена з себе людина в більшості випадків, некритично відноситься до інформації. У цьому стані можна нав'язати або отримати потрібну інформацію. Так діють інтернет-тролі.;
    - ***іронія*** – іронізуючи над думками, вчинками людини, можна спровокувати її вигідну для маніпуляторів поведінку;
    - ***гнів, агресія*** – можна поглибити конфлікт, і в запалі суперечки людина перестає себе контролювати і сповістить потрібну інформацію. Наприклад, про пересування військових чи про нове озброєння.;
- ***байдужість*** – створюється ефект байдужості маніпулятора до теми , співрозмовник буде намагатися довести свою правоту і розкриє потрібну інформацію;
- ***поспіх*** – створюються ситуація, в якій жертва має поспішати, або думати, що часу на вирішення питання дуже мало. Наприклад, знайоме всім: «скидки діють тільки сьогодні» або «товар закінчується»;
- ***підозрілість*** – соціалізація привчила нас, що висловлювати недовіру – погано, і може образити чиїсь почуття. Люди часто соромляться перепитати повноваження маніпулятора або, навіть, жертва намагається виправдати «свою підозрілість», тим самим, розкриваючи інформацію;
- ***довіра до авторитету*** – маніпулятор створює враження, що має права так чинити. Часто, наказ керівника, навіть переданий на словах, має більший вплив, ніж усі попередні правила та навчання;
- ***сліпота до звичних речей*** – люди схильні не звертати уваги на тих, хто виконує свої професійні обов’язки – лікарі, сантехніки,

адміністратори, часто вони навіть не фіксуються увагою жертви, і можуть виконувати будь-які дії не викликаючи підозр чи зауважень;

Уважно на чомусь зосередившись, люди стають практично сліпі, бо не помічають навіть тих стимулів, які зазвичай відвертають їх увагу.

Даніел Канеман

- ***відвертість*** – маніпулятор розповідає співрозмовнику відверту інформацію, у співрозмовника виникають дзеркальні довірчі відносини, що, в свою чергу, спричиняє ослаблення захисного бар'єру, і, як результат, жертва у відповідь теж розкриває потрібну маніпулятору інформацію;

- ***зацікавленість*** – цікавість – це одна з рис людини, яка дозволяє маніпулювати майже будь-якою людиною, головне знайти тему, яка зацікавить жертву;
- ***закоханість*** – у цьому стані людина майже не сприймає інформацію, що не пов’язана з об’єктом закоханості, а сам об’єкт сприймає через «рожеві окуляри». Маніпулювати закоханою людиною, один з найдавніших і найефективніших прийомів.

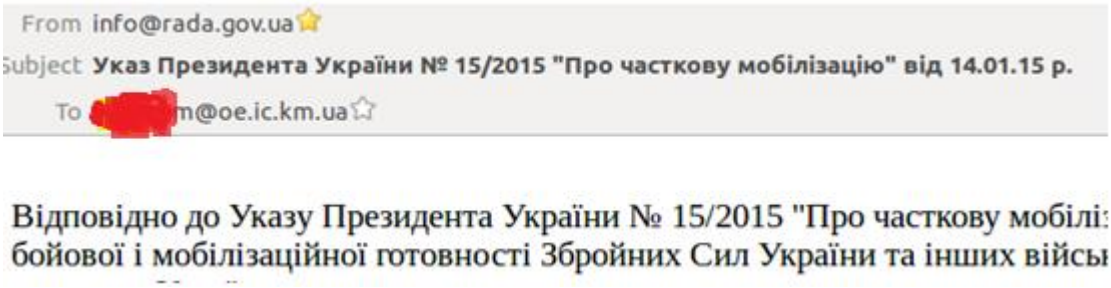
Звичайно, існують і інші методи маніпулювання, але вони менш дієві,або можуть застосовуватись в обмеженому числі ситуацій.

Перелік найпоширеніших способів маніпулювання

Фішинг – Може бути достатньо різноманітним, головною його метою є отримати у жертви конфіденційну інформацію, за допомогою якою можна проводити атаку далі. Це спроба витягнути у жертви пару «логін\пароль» для доступу до банківської системи, або змусити жертву отримати шкідливий інформаційний мем (повідомлення) через підроблені сторінки офіційних установ.

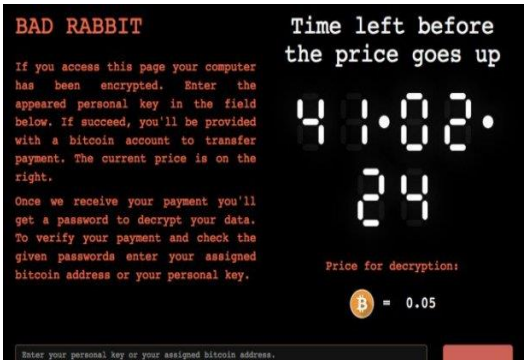
Підробляються зазвичай:

- **сторінки сайту** банку чи іншої установи. Розрахований на неуважних користувачів, які не звертають уваги на дрібниці, помилки, вигляд сторінки тощо.
- **електронні листи** начебто від імені офіційної установи (банку, міністерства…) із запитом.



Фішинговий лист отриманий обленерго під час атаки BlackEnergy начебто з пошти Верховної ради України у прикріпленому файлі містив троянську програму, яку запускали через MS Office з дозволом макросів

- повідомлення про **зараження шкідливими програмами**



Вигляд вікна зі шкідливою програмою

Часто фішінгові атаки поєднують в собі декілька методів маніпулювання, для посилення ефекту, наприклад електронний лист з міністерства інфраструктури (*довіра до авторитету*), містить дуже суворі вимоги до термінів виконання (*поспіх*).

Дослідження показали, що найефективнішим методом соціальної інженерії є повідомлення з фішинговим посиланням: по ньому перейшли 27% одержувачів. Користувачі неуважно читають адресу або навіть просто, не дивлячись, клацають на нього і переходять на підроблений сайт. В деяких випадках користувачі намагалися відкрити файли або ввести пароль за посиланням по 30-40 разів! Іноді адресати повідомляли про те, що лист потрапив до них помилково і пропонували адреси інших людей, кому його слід було б відправити.

Фішинговий сайт – це шахрайський веб-ресурс, який працює під виглядом:

- надання неіснуючих послуг (поповнення мобільного рахунку, переказів з картки на картку),
- веб-ресурсу організації, якій користувач довіряє (клон Приват24, новинної стрічки, урядового сайту).

Більше 90 % фішингових сайтів надають неіснуючі послуги з поповнення мобільного рахунку та переказу коштів з картки на картку

«Емоційна буря» – WOW-повідомлення, наприклад, **«ОГО! Подивись. Я у шоці!»** – «гра» на природній цікавості та емоційності користувачів. Жертва отримує повідомлення від друзів (родичів, з випадкових адрес), зміст яких спонукає перейти за посиланням, відкрити вкладання у е-листі, записатися на у друзі, зареєструватися на форумі, прочитати новину тощо. Як результат можна потрапити у пастку шахрая, де вимагаються конфіденційні дані, потрапити на фішинговий сайт, завантажити шкідливе програмне забезпечення або отримати шкідливий інформаційний мем з новин країни-агресора.

Придорожнє яблуко – підкинути фізичний носій інформації (флеш-накопичувач, тощо), який людина вставить у комп'ютер, і викличе зараження системи, і далі залежно від мети атакувальника, спричинити багато проблем. В цьому випадку, як метод маніпуляції, використовується звичайна цікавість. Таким чином відбулося зараження іранської атомної станції шкідливою програмою Stuxnet, що ледь не викликало ядерну катастрофу.

Зворотна соціотехніка – спонукати людину добровільно попросити про допомогу. В одній з американських компаній на загальний дошці об’яв повісили номер телефону нового електрика, і коли раптово зникло світло, подзвонили за цим номером. Ніхто не поцікавився ні звідки взявся номер, ні особою електрика, що прийшов на виклик. «електрик» не тільки відновив електропостачання, але й встановив у приміщенні засоби прослуховування.

Використання емоцій .Злочинці використовують страх, жадібність, надію і інші емоції для підвищення ефективності своїх атак. Тому в темах своїх листів вони використовують фрази на кшталт «список співробітників на звільнення» (спровокували 38% потенційно небезпечних дій), «виплати премій за рік» (25%) тощо. При отриманні таких повідомлень люди часто забувають про елементарні правила безпеки.

Вороги теж використовують емоційні прийоми для своїх цілей. Антиукраїнська група Миколи Санжаревського збирала гроші для потреб терористів "ЛДНР" через електронні гаманці, які він оприлюднював у дописах в адміністрованих ним групах. Для прикриття

створювались фейкові акаунти і оголошення, що збирають кошти для хворих дітей.

За підозрілими дописами з проханням допомогти грішми можуть приховуватись не тільки шахраї. В таких випадках шахраї то ще півбіди, адже ви не знаєте, можливо вашими зусиллями придбано патрони, якими вбили на війні вашого сусіда по вулиці.

Олена Добровольська

https://enigma.ua/articles/benefis_baleruna_chastina_tretya_ostannya

Захист від атак соціальної інженерії, одне з найскладніших завдань кібербезпеки.

Самі по собі програмні або апаратні засоби, навіть найкращі, не ефективні.

Карикатура з Інтернет

ПРОТИДІЯ

Покладатися можна тільки на власний здоровий глузд, уважність та внутрішнього критика:

- не сприймайте нічого на віру;
- перш ніж прийняти якесь рішення чи виконати дії, вам не властиві, подумайте, а чому ви так робите, порахуйте до десяти;
- ніколи не приймайте рішення під впливом емоцій;
- всю інформацію, що до вас потрапляє – перевіряйте.
- уважно підходите до перегляду е-листів. **Не розпаковуйте вкладені в них архіви, не переходьте за посиланнями, розміщеними в тілі листа**;
- при отриманні підозрілого листа від незнайомого користувача, видаліть повідомлення не відкриваючи;
- якщо підозрілий лист прийшов від вашого знайомого, зв'яжіться з ним і уточніть, посилав він його вам чи ні;

- не відповідайте на підозрілі листи. Відповіддю ви підтвердите, що ваш e-mail «живий». Не грайте на руку зловмисникам;
- користуйтеся антивірусом, за допомогою якого перевіряйте підозрілі листи і прикріплені файли;
- не передавайте свій пароль від електронної пошти третім особам, при: реєстрації, заповненні форм, на прохання для уточнення інформації тощо;
- звертайте увагу на написання адрес сайтів;
- якщо вам пропонують переглянути сайт/фото/відео, з емоційними закликами – не переходьте одразу. Порахуйте до 10-ти та згадайте про соціальну інженерію;
- вводячи логін/пароль в акаунтах на сайтах, звертайте увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру – краще перевірити оригінальність ресурсу ще раз;
- критично ставтесь до електронних листів, а особливо до посилань за якими пропонують перейти незнайомі відправники повідомлень.
- не дивіться російське телебачення.

МІФ 7. СОЦМЕРЕЖІ – ЦЕ БЕЗПЕЧНО (ТАМ ДЕ ВСІ, ТАМ І Я)

Соціальними мережами користуються усі, думають шанувальники цього міфу, отже це безпечне середовище. Ті, хто говорить про небезпеку соціальних мереж – темні і відсталі люди, які не розуміють сучасного світу.

Насправді

Розвиток сучасних технологій дозволяє обмінюватись інформацією з різними людьми, з різних країн, з різними уподобаннями. Самі по собі соціальні мережі, як засіб обміну інформацією, дуже корисні. Проте треба чітко розуміти, які дані виставляються у соціальних мережах, як їх може використати зловмисник, і як їх можна використати у рамках інформаційної війни.

АНАЛІЗ ЗАГАЛЬНОДОСТУПНОЇ ІНФОРМАЦІЇ

Розміщуючи інформацію про себе в соціальних мережах, ви повинні бути готові до того, що її може побачити велика кількість людей. І ваше приватне життя стає надбанням громадськості.

Активні користувачі соцмереж подають свою конфіденційну інформацію, анітрохи не замислюючись над тим, що її можуть побачити :

- сторонні люди,
- спецслужби,
- колектори боргів,
- роботодавці,
- родичі,
- особи, перед якими не хотілося б афішувати своє життя.

В 2017 році 19-річний українець Павло Гриб поїхав до Білорусі на зустріч з дівчиною, з якою познайомився у мереж ВКонтактє. Коли від нього тривалий час не було звісток, батьки занепокоїлись і почали шукати сина. Павло «знайшовся» у СІЗО на території Російської Федерації. Його викрала ФСБ. Батько Павла розповів ЗМІ, що на сина вийшли через моніторинг соціальних мереж. Хлопець не брав участі в бойових діях. Він активно писав у соціальних мережах, не приховуючи свого ставлення до російської агресії. На час написання посібника Павло Гриб є одним з російських бранців.

Навіть якщо людина не настільки активна, як Павло, соціальні мережі можуть бути небезпечними. Згідно зі статистикою близько половини пограбувань будинків в США відбувається після того, як злодії вивчають сторінки жертв в соціальних мережах. Інформація, яку можна знайти там, вражає – від хобі та розпорядку життя людини до її добробуту. Навіть така невинна інформація, як фото кішки, може вказати зловмиснику, що кішка породи мейкун, вартість від 500 доларів, а отже хазяїн (хазяйка) заробляє чимало. Переглядаючи фото можна зробити висновок, чи людина самотня, чи живе з великою кількістю родичів, якщо дитина ходить до дитячого садочку, то ймовірно, до обіду дома нікого не має, а геопозиціонування на фото вкаже точну адресу квартири, де лежать гроші.

Міф 7. Соцмережі – це безпечно

Ви можете розміщувати інформацію про колег або свого боса, яка вам здається невинною, але їх погляд на це може відрізнятися від вашого. Все може закінчитися розголошенням конфіденційної інформації, що дискредитує вас і призведе до серйозних наслідків. Можна розмістити інформацію про себе, яка, на ваш погляд, ніяк не пов'язана з роботою. Як би там не було, але якщо ви соціальний вузол, то ви невільні в розміщенні особистої інформації в мережі.

Поки ви не приєдналися до соціальних мереж, ви можете відділити ваше особисте життя від роботи, але активність в соціальних мережах, всупереч вашим бажанням, все одно з'єднає їх.

Старанному і цілеспрямованість зловмиснику не складно отримати з розрізнених публікацій достатньо відомостей, щоб провести успішну фішингову атаку проти колег (друзів, родичів) об'єкта. Для присипляння пильності досить повідомити в шахрайському листі якісь подробиці, які, здавалося б, може знати тільки об’єкт. Проте розкопати ці дані можна багато де, аж до фотографій з офісу або з пікніка.

Все більше і більше роботодавців використовують соціальні медіа для того, щоб прояснити минуле своїх претендентів. Ви можете бути студентом або спокійно працювати на вашому нинішньому місці. І, можливо, ви навіть не підозрюєте, що скоро будете шукати нову роботу. Ви можете у будь-який момент видалити свої дані, але це не значить, що вони не залишились у ваших друзів, або інших зацікавлених осіб. І будь-яка надмірно відверта або компрометуючий вас інформація стане відомою будь-якій зацікавленій особі.

Держдепартамент США у 2018 р. запропонував проект нових правил для гостей і іммігрантів, що приїжджають в США. Згідно з ними при перетині кордону доведеться надати історію записів в соціальних мережах, а також розкрити інші подробиці. Правила вводяться, як одні з ключових заходів щодо підвищення безпеки, відповідно до розпорядження Президента Трампа про «екстремальні перевірки» для боротьби з незаконною імміграцією і тероризмом.

Збираючи дані про користувача фото, народження, інформацію про сім'ю, роботі, улюблених фільмах та книгах, подорожі, коло спілкування, місця проживання тощо, зловмисники можуть скористатися цими даними для створення ще одного облікового запису – віртуального двійника. А далі розміщувати повідомлення від імені користувача, наприклад відомого волонтера, і збирати кошти.

АНАЛІЗ ПРОФІЛЮ КОРИСТУВАЧА

Соціальні мережі зберігають інформацію про кожного користувача, про всі його дії в його обліковому записі, а також дії, що не стосуються його облікового запису. Не так давно соціальні мережі були змушені повідомити про те, які саме дані вони зберігають, і на щастя з 2018, після багатьох скандалів, навіть дозволили видаляти свої дані повністю (принаймні офіційно).

Пост про те, яку інформацію збирає про користувачів Facebook

Для чого ж збираються всі ці дані? На їх обслуговування витрачаються мільярди, навіщо це потрібно.

У міфах 2 та 3 було розглянуто, наскільки сучасний світ залежить від обробки великих даних, і соціальні мережі, по своїй суті, стали тими великими даними, що дозволяють заробляти величезні гроші.

І в першу чергу – це реклама та просування товарів. Соціальні мережі мають механізми, що дозволяють стороннім розробникам отримувати дані, що зберігаються в профілі користувача (не тільки, те що відображається на сторінці). А отже вивчати уподобання користувача, що він читає, за яку партію голосує, до якого кафе ходить, в якому супермаркеті купую молоко і якої фірми, стало дуже легко.

Але так само ці дані можуть передаватися для політичних цілей або в рамках ведення інформаційної війни.

Згідно з опублікованими документами, Фейсбук збирає наступну інформацію:

- час, частоту та тривалість активності в вікні з вкладкою соцмережі (включаючи інформацію про те, відкрито воно або перебуває у фоновому режимі);
- покупки, здійснені на сторонніх сайтах;
- плагіни в браузері користувача;
- рухи курсору на пристрої;
- використання камери, вбудованої в додаток Facebook;
- метадані фотографій (включаючи час і місце зйомки);
- встановлені додатки;
- назви і типи файлів на пристрої користувача;
- ідентифікатори додатків;
- кількість вільного місця на пристрої;

- контакти з довідника користувача;
- журнал дзвінків і історію SMS з Android-пристроїв;
- найближчі точки доступу Wi-Fi і стільникового зв'язку;
- інформацію мобільних і стаціонарних провайдерів через комп'ютери, телефони, зв'язані телевізори та інші пристрої в мережі;
- рівень заряду пристрою;
- параметри та дозволи на пристрої;
- інформацію та фотографії інших користувачів, а також частоту взаємодія і спілкування з ними.

У Facebook додали, що також можуть отримувати інформацію про користувачів від сторонніх компаній. Мова йде про дії як в онлайні, так і в офлайні, але про які саме – представники компанії не уточнили.

Додатки, які використовуються на мобільних пристроях для роботи з соцмережами мають доступ до:

- користувацького ID, ім'я, фото профілю, адресу е-пошти, номер телефону та місце розташування користувача.
- імен та ID всіх користувачів, з якими власник смартфона обмінюється повідомленнями.
- даних про друзів користувача: ID, дата народження, історія роботи і освіти, і чи вони зараз онлайн.
- дані про друзів його друзів.

Приватна компанія з аналізу даних Cambridge Analytica отримала дані приблизно 50 мільйонів користувачів соціальної мережі. Це стало можливим завдяки програмі thisismydigitallife, яку в 2014 році створив Олександр Коган, професор Кембріджського університету Великобританії.

В 2012 році дослідник Міхал Козінський довів, що аналізу 68 лайків у Facebook достатньо, щоб визначити колір шкіри людини (з 95% ймовірністю), її гомосексуальність (88%) та прихильність до Демократичної чи Республіканської партії США (85%).

Після 70 проаналізованих лайків система знатиме про вас більше за друга, а після 150 – більше за батьків.

Донедавна будь-який розробник, що хотів аналізувати дані з соціальних мереж, міг просто зареєструватися на сайті з підтримки та отримати токен, що надавав йому право отримувати персональні дані користувачів соцмереж. І якщо Facebook та Twitter на сьогоднішній день, під впливом громадськості, закрили ці токени майже для всіх невеликих компаній (залишились, наприклад виробники обладнання), то деякі соціальні мережі (ВКонтакте) й досі надають доступ до сторінок користувачів без обмежень.

ОСОБЛИВОСТІ ДОСТУПУ ДО ІНФОРМАЦІЇ З БОКУ СПЕЦСЛУЖБ

Соціальні мережі зберігають інформацію про всі дії, що відбуваються на сторінці, і нічого не видаляють.

Доступ до цієї інформації може надаватись і надається спецслужбам залежно від законодавства держави, в якій зареєстрована соц. мережа.

І якщо щоб отримати персональні дані з соціальної мережі Facebook, спецслужбам необхідно отримати постанову суду в США (навіть якщо це спецслужби України), то з 2015 р. доступ до всіх соціальних мереж у РФ здійснюється напряму від агентів ФСБ.

Постанова № 327 від 8 квітня 2015 р. надає доступ до персональних даних користувачів Роскомнадзору (всі ресурси в Інтернет та всі інформаційно-телекомунікаційні системи) для співробітників ФСБ Російської Федерації.

Громадяни України масово не розуміють, що вони передають до ФСБ вразливі дані, як і не усвідомлюють, яким чином ці дані будуть використані.

«Хтось із сторонніх міг постраждати, цього я не знаю. У мене була сторінка «ВКонтакте», мені писали люди, пропонували допомогу, дівчинка якась писала, і при мені вони від мого імені, маючи мій телефон, поміняли пароль, тут же увійшли, і жінка-кат при мені листувалася з нею. Від мого імені вона списувалася з тими, хто пропонував допомогу. Ось це мені вже невідомо, постраждали люди чи ні.».

Сергій Захаров, малював карикатури на діячів терористичних угруповань на вулицях Донецька

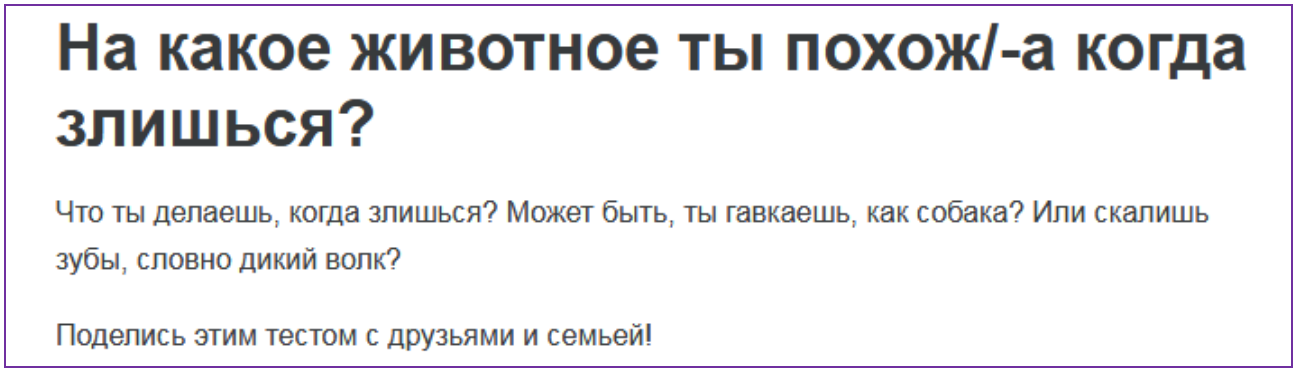
http://www.radiosvoboda.org/content/article/26646944.html

Та незважаючи на численні роз’яснення, попередження і заборони, є випадки використання російських сервісів для листування та інформування в державних і бюджетних установах. Рівень усвідомлення загроз втручання РФ у всі види пристроїв, підключених до Інтернет, в суспільстві не виріс. Державні інституції мало ведуть роз’яснювальну роботу навіть для державних службовців про загрози безпеки, пов’язані з користуванням російськими Інтернет сервісами, максимум розсилають вказівки не користуватися певними сервісами на роботі і не перевіряють їх виконання.

Використання російських сервісів значно полегшує роботу інтернет-зловмисників проти України, спецслужбам навіть не потрібно вигадувати віруси, аби отримати паролі і доступ до скриньок, законодавство Російської Федерації дозволяє їм зробити це в якнайшвидші терміни.

ТЕСТИ – ЦЕ ВЕСЕЛО

Багато користувачів вважають тести у соціальних мережах гарною розвагою. На кого з кіноакторів ви схожі? Ким ви були в минулому житті? Що на вас чекає у наступному році? Відповідь на ці важливі питання дадуть тести, і, навіть якщо це неправда, можна посміятись і обов'язково поділитись з друзями радістю.



Приклад тесту з Інтернет

Тести використовуються для збору і аналізу даних про користувачів.

Російські пропагандисти використовують тести в інформаційній війни для впливу на українських громадян. Як це відбувається?

Щоб вплинути на людей, потрібно знати, на що вони реагують. Інформаційні атаки українців в 2014 році історіями про розіп'ятих хлопчиків не досягли бажаного ефекту. Більша частина української аудиторії не тільки не повірила у вигадані страхіття, але й почала уникати маніпулятивного впливу російського телебачення. Тому пропагандисти з Росії почали досліджувати соціальні мережі, аби з'ясувати, що люди коментують, яку роль відіграють у своєму кластері і як їх оточення пов'язане з іншими групами.

Досвідчений психолог може створити психологічний портрет людини, вивчивши її профіль у соціальних мережах. Але як створити «портрет» спільноти? Потрібно багато досвідчених психологів, багато часу і багато грошей.

Використати тести – простіший і швидший шлях. Найкраще, коли людина дасть відповідь одразу на кілька тестів. На основі цих відповідей створюється простий, але достовірний психологічний портрет, з врахуванням зв'язків та ролі у спільноті (комунікативному кластері).

Наступний крок – підготовка орієнтованого на людей у конкретній спільноті інформаційного продукту, наприклад, фейкових повідомлень певної тематики. Наприклад, для волонтерів – інформація про розкрадання волонтерської допомоги, для чоловіків-військовозобов'язаних – фейк про заборону виїзду за кордон, для літніх людей – страшилка про похорони за рішенням суду. Таке повідомлення подається від імені «експертів», які, знову ж

таки підібрані на основі вподобань спільноти. Часто «експертами» виступають «знайома нотаріус», «сусідка випадково почула», «екс-радник голови фонду невідомо чого». Далі повідомлення посилюється і передається цілком добросовісними коментаторами, які своїми емоційними коментарями «влада хоче нас знищити», «зовсім про людей не думають», «продались зверху до низу» підсилюють негативний вплив на спільноту. Кількість негативних коментарів швидко зростає, і врешті – доходить до інформаційного «вузла» кластера і через нього передається на весь кластер, створюючи настрій відчаю і недовіри. Через посередників-коннекторів маніпулятивне повідомлення передається в інші кластери, поширючи «зраду» в українському суспільстві.

Відповідати на тести, які невідомі особи пропонують з невідомою вам метою, означає полегшувати роботу маніпуляторам. Все, що ви повідомите, може бути використане і вже використовується проти вас.

ПРОТИДІЯ

Розміщуйте на сторінках у соціальних мережах якомога менше конкретних даних про своє життя.

Не публікуйте інформацію, за якою можна визначити вашу домашню адресу і час, коли там нікого не буває.

Не ставте в загальному доступі пости про дорогі покупки або справи, в результаті яких можна зробити висновок про наявність у вас великої суми грошей або цінностей, які можна перепродати.

Не описуйте свій постійний маршрут, (між домом – та роботою, школою чи спорткомплексом, що ви відвідуєте) – напади з метою пограбування не завжди бувають випадковими.

Не повідомляйте куди і як надовго ви їдете, а якщо без цього не можливо, додайте приписку про родичів, що будуть в цей час у вас жити або про включену охоронної сигналізації (навіть якщо це не правда) – це напевно відлякає любителів легкої наживи.

Використовуйте здоровий глузд, коли ділитеся своєю особистою інформацією з іншими. Будьте готові до того, що ваша сторінка в будь-який момент може стати надбанням громадськості.

Не використовуйте соціальні мережі, які працюють на РФ.

Не ходіть на ресурси, які співпрацюють з РФ в плані надання доступу доданих.

Ігноруйте тести в соціальних мережах.

Поширюйте інформацію про шкідливість тестів в своїх спільнотах.

МІФ 8. В МЕНЕ Є АНТИВІРУС – МОЇ ДАНІ В БЕЗПЕЦІ

Люди, які вірять в цей міф, думають, що встановивши антивірусну програму, вони захищають свій комп'ютерний пристрій надійно і назавжди. Антивірусна програма може бути придбана офіційно або скачана з Інтернет, або подарована сусідом – не має значення, вона в будь-якому разі захистить. Щодо загрози кібератаки з боку Росії, то це вигадка влади, аби відвернути увагу українців від високих цін на комунальні послуги чи стану доріг.

Насправді

Антивірусні програми – це ліки, але не панацея. Встановлення антивірусної програми не гарантує безпеку комп'ютера!

Антивірусні програми:

- пишуть люди, вони можуть помилятись;
- так само як інші програми, мають вразливі місця;
- вразливі місця можуть бути використані для атак на систему;
- навіть проти найкращих антивірусних рішень продаються експлойти (програми, що використовують різні вразливі місця для атак на систему);
- статистика кібератак за 2017 рік показала, що різноманітні техніки взлому використовувались у 62% випадках. У 51% випадків злочинці використовували шкідливі програми, в інших випадках застосувались інші інструменти, зокрема соціальної інженерії (див. міф 6). Майже половина кібератак відбулась із застосуванням технологій, від яких не захищають антивірусні програми.

КІБЕРАТАКИ – ЦЕ ЕКОНОМІЧНО ВИГІДНО

Кібератаки – це прибутковий нелегальний бізнес світового рівня.

Прибутки від кібератак перевищують прибутки від незаконного обігу наркотиків та зброї.

З поширенням методів інформаційних воєн з'явилися цільові кібератаки, метою яких є не стільки заробляння грошей, скільки гібридні військові дії проти різних країн та компаній. Андрій Парубій, аналізуючи можливі загрози у гібридній війні Росії проти України, ще в 2014 році визначив кібератаки як одну з основних загроз.

Одночасно фахівці, що спеціалізуються на кібербезпеці, зареєстрували зростання кількості кібератак на інформаційні системи в країні. Жертвами російських кібератак стали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, громадські активісти.

Після початку російської агресії кількість кібератак виросла і змінився їх характер. Якщо на початку їх мета полягала в отриманні інформації, то потім починаючи з 2014 року атаки спрямовані на виведення з ладу енергосистем України, транспортних комунікацій, державних установ, що може спричинити не тільки економічні збитки, але й серйозну дестабілізацію в країні.

23 грудня 2015 року зафіксована перша в світі підтверджена кібератака на енергосистеми, і сталася вона в Україні. В результаті дій хакерів споживачі

«Прикарпаттяобленерго» залишались без світла від однієї до шести годин. Атака відбувалась із використанням троянської програми BlackEnergy. Одночасно були атаковані «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. Підключення зловмисників до інформаційних мереж відбувалося з підмереж, що належать провайдерам в Російській Федерації.

Протягом 2017 рік трапилось три кібератаки світового рівня:

- WannaCry 

- NotPetya 

- BadRabbit 

Вірус NotPetya з’явився в 2016 році, а 27 червня 2017 відбулось його масове поширення. 75% постраждалих від атаки комп’ютерів – українські. Вірус атакував українські енергетичні кампанії, банки, аеропорт, урядові сайти, Чорнобильську АЕС, київський метрополітен. Маскуючись під вимагача, вірус вимагав за відновлення доступу до даних 300 доларів в біткоїнах. Уряди США, Великобританії, Австралії, Данії, Канади та України поклали відповідальність за атаку на Росію.

Одночасно з атаками на комп’ютери зростає частка шкідливих програм для мобільних пристроїв. Їх розробники використовують особливість мобільних операційних систем, яка дозволяє завантажувати та встановлювати програми, покладаючись на уважність користувачів. Величезна кількість програм, що розповсюджуються через легальні Маркети Android та iOS, мають недокументовані функції (а іноді і описані, але хто ж читає), які дозволяють красти персональні дані, реквізити платіжних систем, геопозиціонування, а також прослуховувати всі розмови і трафік, фотографувати та робити відео без згоди користувача.

Троян Skygofree може відслідковувати місцезнаходження пристрою та включати запис звуку в той момент, коли його власник знаходиться у певному місці.

Дієвість, ефективність та прибутковість кібератак можна підтвердити такою цифрою. Протягом 2017 року, в середньому виявляло до **285 000** нових зразків шкідливих програм **щоденно**. Причому більшість з них змінюються при кожному новому зараження, використовуючи так звану техніку поліморфізму.

В Україні, та і у більшості світу, кібератаки показали фактичну відсутність безпеки в різних автоматизованих системах, незважаючи на наявність антивірусних систем.

А якщо є запити, то є і пропозиція.

ДЕ БЕРУТЬСЯ ШКІДЛИВІ ПРОГРАМИ

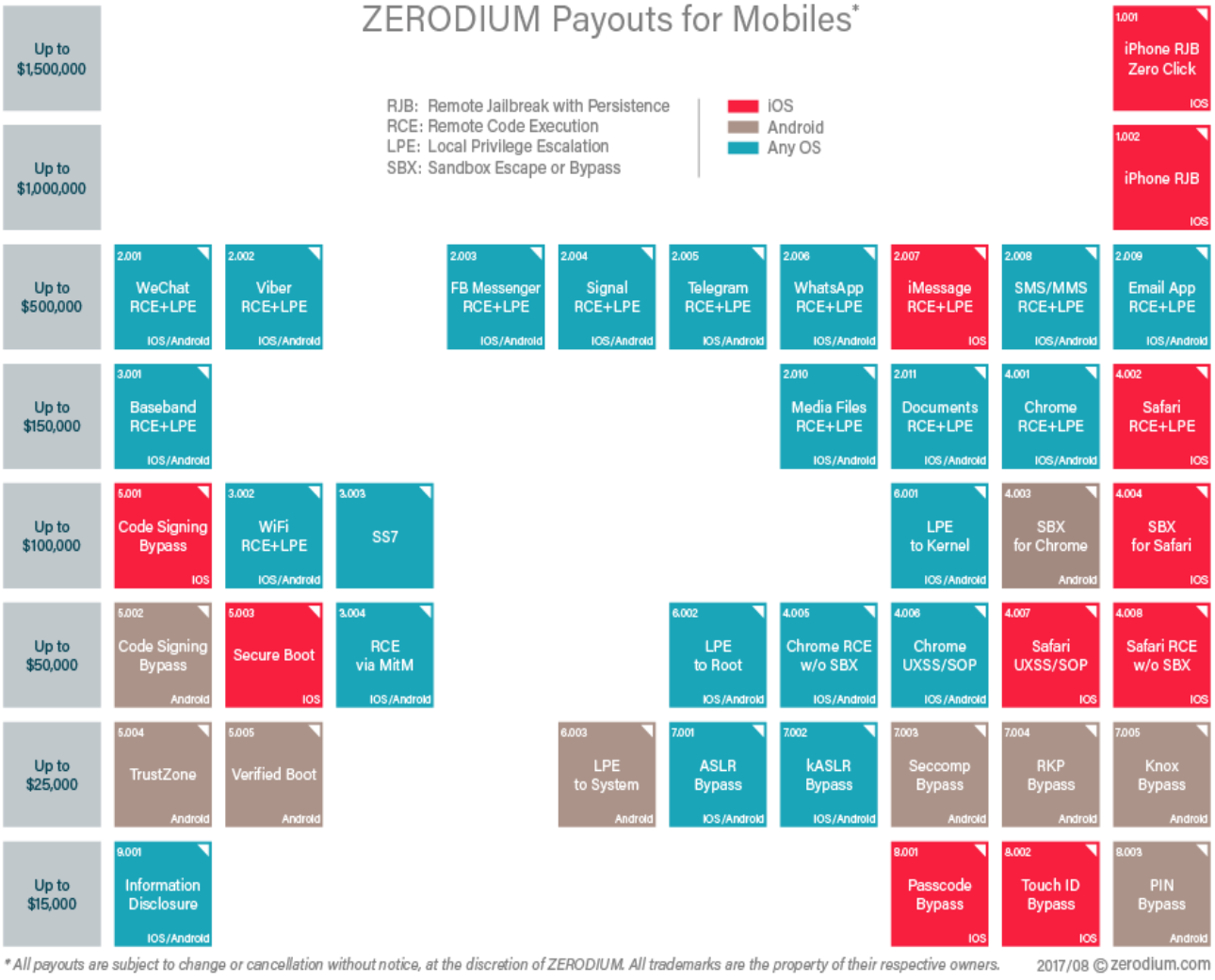
Шкідливу програму можна написати самому, але для цього необхідно мати серйозні знання в галузі інформаційних технологій, програмування, мереж, операційних систем і багато чого іншого. Людей, які здатні написати працюючий шкідливий додаток не так вже й багато, їх зазвичай називають хакерами. Вони можуть працювати на себе, і розповсюджувати шкідливий код заради «мистецтва», але таких стає все менше. Зазвичай сучасні хакери або працюють на спецслужби (наприклад, АНБ США, ФСБ РФ тощо) або на «темну сторону», заробляючи на цьому непогані фінансові статки.

Для того, щоб перейти на «Темну сторону» користувач має встановити спеціальний додаток, наприклад, Tor, який після інсталяції повністю шифрує всю активність в Інтернет. Спочатку такі системи створювались для анонімності користувача, але часто анонімність плутають із вседозволеність, і почали розвиватись анонімні мережі, називають їх по-різному: darknet, hidden sevices, deepweb.

З часом darknet почали використовувати для розповсюдження незаконних товарів, в тому числі і шкідливого програмного забезпечення. Є цілі площадки та аукціони, на яких можна купити шкідливий код, або вразливість нульового дня (так називають вразливість інформаційних систем, яка ще не відома, і, проти якої не розроблені механізми захисту). Ціна буде залежати від багатьох факторів, в тому числі від того, чи виявляють цей код антивірусні програми. Ціни на вразливості нульового дня стартують від кількох десятків тисяч до півтора мільйона доларів.

Здається це дуже дорого, але коли мова йде про мільйони, що можна заробити на зламі інтернет-банкінгу, або про престиж держави, або про

операцію у ході інформаційної війни, тоді розумієш наскільки просто і легко обійти антивірусні рішення.



Вартість різних експлойтів для різних операційних систем

Наприклад, вразливість, що використовували для зараження комп'ютерів під час епідемії WannaCry, була розроблена спеціалістами АНБ США, для контролю за комп'ютерами терористів (офіційна версія) і після взламу продавалась на темній стороні за дуже великі гроші.

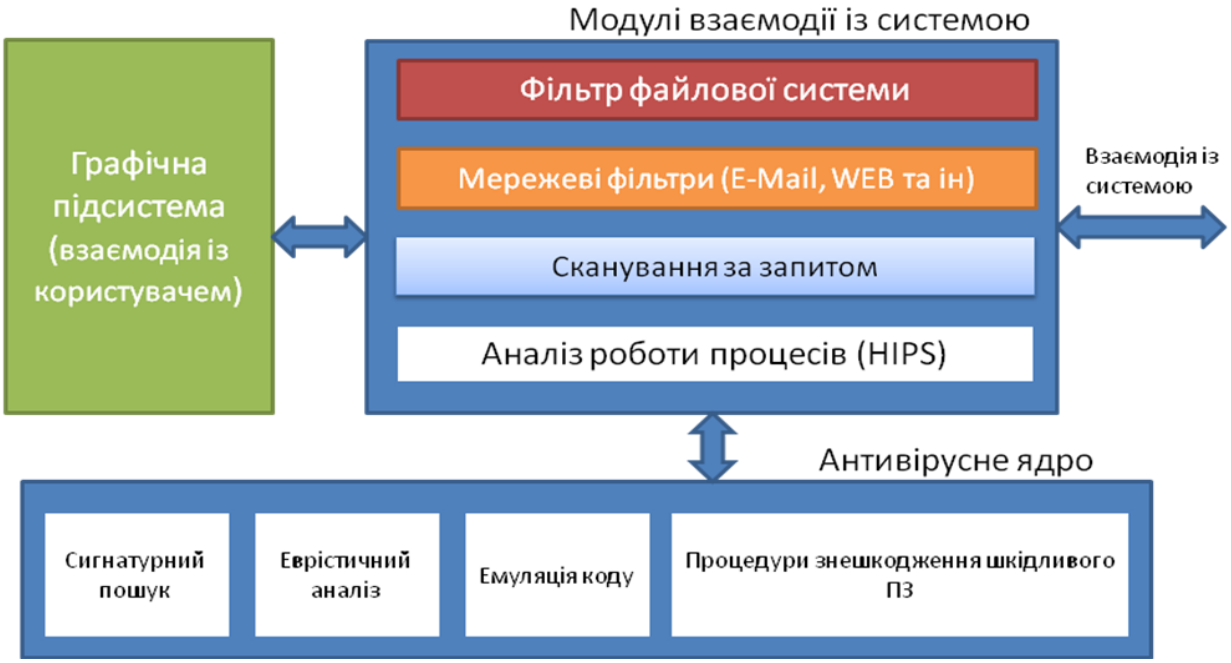
До речі цю ж вразливість частково використовував і NotPetya, і BadRabbit і низка інших менш відомих шкідливих програм.

СТРУКУТУРА АНТІВІРУСУ

Іншою проблемою, яка зумовлює обхід шкідливим засобами антивірусних систем, це сама природа їх роботи.

Основною частиною будь-якого антивірусу є не гарний інтерфейс, а антивірусне ядро, яке і відповідальне за виявлення та знешкодження шкідливих програм. Більшість антивірусів використовують два види пошуку та аналізу

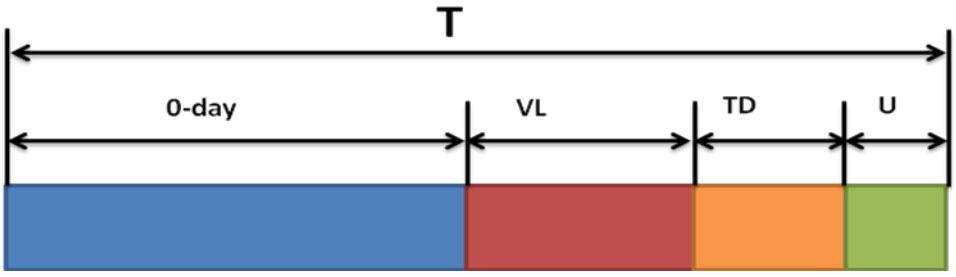
шкідливих програм: сігнатурний та евристичний. Перший шукає підозрілі ділянки в коді програм (наприклад напис «This is virus», і таке є), а другий виявляє підозрілу активність (наприклад навіщо пасьянс намагається отримати доступ до поштової скриньки користувача).



Узагальнена схема антивірусних систем

Комбінація цих двох підходів, здається, дозволяє виявляти всі можливі ситуації з появою шкідливої програми. Проте, часто шкідливі програми не мають постійної сигнатури, за якої її можна ідентифікувати, а евристичні методи обходить шляхом приховування своєї активності або отриманням дозволу від користувача.

Крім того, для того, що б антивірус зміг використати сигнатуру, її має хтось написати і додати в базу сигнатур.



Життєвий цикл розробки антивірусної сігнатури

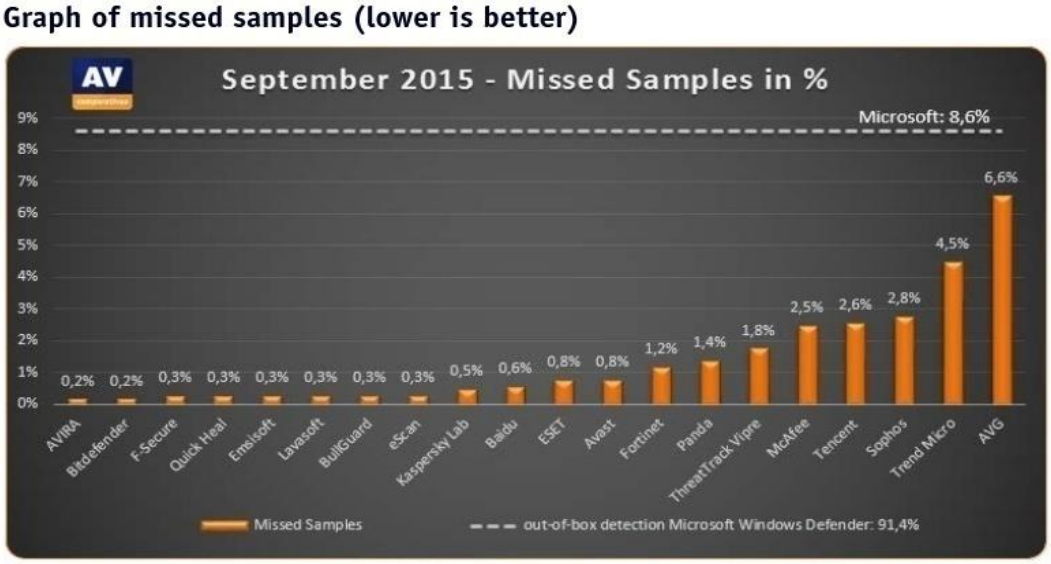
- 0-day – період від моменту появи вірусу в дикому вигляді до потрапляння його до антивірусної лабораторії;
- VL – час роботи вірусної лабораторії;
- TD – технологічні затримки (тестування запису);
- U – період оновлення вірусних баз.

Час потрапляння антивірусного запису з моменту появи вразливості може складати роки (наприклад виявлена нещодавно вразливість у MS Office з'явилась у 2000 році і з тих пір 17 років залишалась не відомою, і станом на 2018 р. не виправленою). Ще додатковий час потрібний для знаходження особливих сигнатур, що допоможуть виявляти шкідливу програму, ще час на тестування та перевірку. А потім необхідно чекати поки користувач, нарешті, оновить бази сигнатур.

В той час як зловмиснику з моменту написання програми потрібно лише кілька годин або днів.

ТЕСТУВАННЯ АНТИВІРУСІВ

При виборі антивірусного рішення, часто переглядають статистику, як той чи інший антивірус виявляє шкідливі програми. Найкращі з них показують трохи більше ніж 90 % на тестових вибірках.



Статистика за пропущеними шкідливим програмами у різних антивірусів

Отже, при появі до **285 000** шкідливих програм щоденно (статистичні дані за 2017 р.), 28 500 з них залишаються не виявленими навіть найкращими антивірусними рішеннями.

Крім того, існують різні «тестові вибірки». Розрізняють «велику тестову вибірку» та «малу тестову вибірку». Велика, відповідно, містить всі зразки шкідливих програм, які колись існували, Мала – тільки ті, що є актуальними протягом останніх кількох років. Тестувати весь час на Великій виборці – витратно за часом та ресурсами (крім того більшість з прикладів навіть не зможуть запуститись на сучасних системах), але тестування на Малій, дозволяє зловмисникам просто реанімувати актуальні колись шкідливі програми. Ну і звичайно, кожен дослідник і лабораторія, мають свої «актуальні вибірки», за якими антивіруси і показують свої найкращі результати.

Але будь-яка вибірка, не дозволяє перевірити антивірусне рішення в реальних умовах. Жодна антивірусна компанія не показує результати тестів при так званому «дикому вході в Інтернет», коли антивірус змушують працювати в реальному світі з користувачем, який заходить на всі посилання та завантажує все підряд. Тут результати навіть найкращих антивірусів дуже низькі.

ОСОБЛИВОСТІ ПРАВ ДОСТУПУ АНТИВІРУСІВ ДО ІНФОРМАЦІЇ НА ПК

Дослідження антивірусних версій продуктів Kaspersky Antivirus показало:

- *всі продукти антивіруса Касперського працюють в системі з найвищим пріоритетом, і не можуть бути обмежені або контролюватися будь-яким зовнішнім програмним забезпеченням або самою операційною системою.*
- *під час роботи продукти проводять обмін даними з серверами, розташованими в США і Росії.*
- *всі дані, що передаються, відправляються з комп'ютера зашифровані і не можуть бути проаналізовані.*

https://ain.ua/2014/05/27/eksklyuziv-chem-grozit-ispolzovanie-antivirusa-kasperskogo-v-organax-gosudarstvennoj-vlasti

Фактично аналіз майже будь-якого антивірусного рішення може містити ті самі результати. Що вони означають?

По-перше, будь-який антивірус має найвищі привілеї в системі, а отже може читати будь-які дані, виконувати будь-які команди, запускати додаткові програми. І все це без дозволу користувача чи інших систем. Навіть якщо розробник не має на меті щось погане, існуючими вразливостями може скористатись зловмисник. Крім того, багато шкідливих програм видають себе за безкоштовні або зламані антивірусні програми, заохочуючи користувача самого ставити собі шкідливу програму.

По-друге, антивірусні рішення повинні постійно оновлювати свої бази, проте, що надійде в наступному оновленні, не знає ніхто. Це може бути легальне оновлення, яке з різних причин може видалити улюблену програму, оскільки нова сигнатура містить схожий запис. Так само в сигнатурах може бути умисно вписана, наприклад, фраза «НАКАЗ міністерства фінансів України» і, як результат всі файли з таким написом будуть знищені.

По-третє, для покращення алгоритмів роботи антивірусні засоби збирають багато інформації про систему, додатки та механізми, що в ній встановлені, мережеві ресурси (і це тільки те, що вказано офіційно) тощо, а потім надсилають її до центру обробки у хмарних сервісах виробника

антивірусу. Оскільки ці дані зашифровані користувач не може перевірити, що саме передається (паролі, скріншоти, натиснуті клавіші?).

ПРОТИДІЯ

- Не відкривайте вкладень до е-листів, якщо
  - автор з невідомих причин змінив мову спілкування;
  - тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим тощо;
  - повідомлення з нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів і т.ін.).
- Не дозволяйте запуск макросів.
- Не надавайте привілеї невідомим програмам.
- Не переходьте за посиланнями в листах, соціальних мережах тощо.
- Забороніть встановлення програм з облікового запису користувача.
- Робіть резервні копії своїх документів.
- Не використовуйте чужі флешки.
- Не вставляйте свої флешки в чужі комп'ютери.
- Слідкуйте за назвами сайтів, на які переходити (фішінгові сайти).
- Не качайте файли з файлообмінників.
- Не відкривайте архіви (особливо ті, що саморозпаковуються).
- Використовуйте тільки перевірені антивірусні рішення від довірених виробників.
- Не використовуйте заборонені антивірусні продукти, взламані, або неліцензійні.

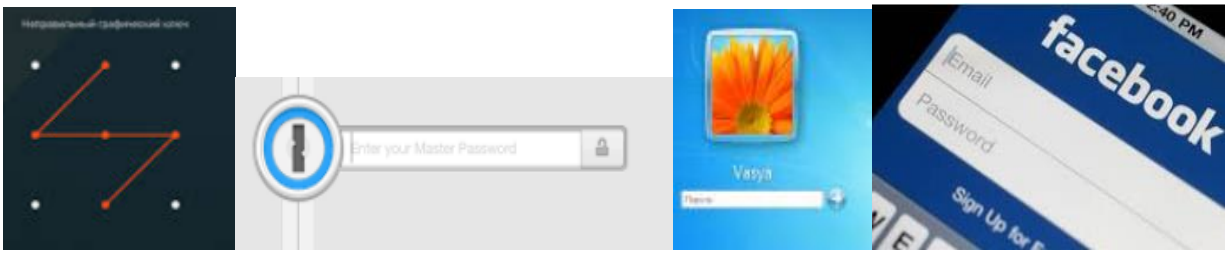
МІФ 9. МІЙ ПАРОЛЬ НІХТО НЕ ВГАДАЄ АБО НАВІЩО ТІ ПАРОЛІ

Цей прекрасний міф має мільйони шанувальників у всьому світі. Люди вважають, що пароль – незначна дрібниця, вигадана, щоб ускладнити їх життя. Найкраще рішення – запам'ятати в програмі, мати однаковий пароль для всіх сервісів, і ніколи не змінювати. Пароль має бути простим. «Навіщо мудрувати, напиши дату свого народження» – радять новачкам.

Але є особливо просвітлені – ті, хто вважає власний пароль унікальним творінням, стійким до будь-якого чужого втручання.

Насправді

Паролі використовуються для входу у комп'ютер (обліковий запис), доступу до електронной пошти, соціальних мереж, інтернет-банкінгу тощо.



Різноманітні форми для парольної автентифікації

Неможливо уявити комп'ютерні системи, в яких би не використовувались послідовності знаків, які потрібно запам'ятати.

І це напевне найбільша проблема всіх парольних схем захисту – як не забути власний пароль.

ШОКУЮЧИ ФАКТИ ПРО ПАРОЛІ

Люди в усьому світі використовують однакові паролі.

Найулюбленіший пароль усіх часів та народів – *qwerty*. Його може запам'ятати будь-хто (це перші шість літер на верхньому рядку англомовної розкладки клавіатури). Крім *qwerty* існує десятка найпопулярніших паролей за різні роки. У 2017 році Топ10 паролів був такий:

23456;	*1234567890;*
123456789;	*1234567;*
qwerty;	*password;*
12345678;	*123123;*
111111;	*987654321;*

Такі паролі небезпечні тим, що їх знають всі, і, відповідно, зловмисники теж. Підібрати їх, і взламати Вашу електронну пошту або інтернет-банкінг не є проблемою.

Перевірте чи Ваш пароль є у цьому списку?

Для створення паролів використовують особисті дані

Особисто автор довгий час отримувала доступ до Інтернету використовуючи дату народження адміністратора. На жаль, це поширена практика. Користувачі вірять в міф 2 (про мене ніхто нічого не знає), забуваючи, що самі надають доступ до власних даних через соціальні мережі, онлайн тести, заповнюючи анкети у магазинах.

Найбільш поширеними особистими паролями є:

дата народження,
прозвисько собаки, кішки
ім'я коханої (коханого) тощо

ну і як же без самого таємного

дівоче прізвище матері

Ви ще використовуєте такий, пароль? Тоді швиденько його поміняйте.

В сучасних системах часто є суворі вимоги для паролів

Наприклад, паролі повинні:

- містить великі та малі літери;
- містить цифри і символи;
- більше 8 символів довжиною;
- не є словом ні на одній з мов, діалектів, жаргонів, сленгу тощо.

Задля вашої безпеки дотримуйтесь цих вимог!

Програми–генератори паролів не гарантують безпеки

Вони можуть підібрати пароль, що відповідає умовам системи і легко запам'ятовується. Але зловмисник теж має такий генератор, і може брати паролі для підбору з нього.

Вразливим місцем паролів є використання одного і того ж паролю для різних потреб, не залежно від важливості

Придумавши вдалий пароль користувач починає використовувати його всюди, для входу на домашній комп'ютер, для від інтернет-банкінгу і для реєстрації на форумі садоводів-любителів. Зрозуміло, що останній не використовує механізмів захисту паролів, і, скоріше за все, доступ до них може отримати майже кожен бажаючий, а далі стає можливим взлам і електронної пошти, і інтернет-банкінгу.

При використанні однакового паролю дуже легко потрапити до пастки шахраїв, і тим самим відкрити доступ до ВСІХ своїх ресурсів.

Паролі складно запам'ятати? Що ж, будемо записувати!

Складність запам'ятовування великої кількості паролів, ще й вимога їх періодично міняти, призводить до іншої проблеми – записування паролів.

Для того, щоб не забути пароль, його записують

- на стікері та чіпляють до монітору;
- на папірці і кладуть під клавіатуру;
- у файлі на комп'ютері;
- електронній пошті тощо.

Закінчується це погано

13 січня 2018 року жителі Гаваїв налякали фальшивим повідомленням про запуск балістичної ракети по островам. Паніка продовжувалась близько 40 хвилин, поки не було розіслано офіційне скасування. Повідомлення про атаку було передано через системи оповіщення департаменту з надзвичайних ситуацій штату Гавайї. А за кілька день до атаки у ЗМІ було показано інтерв'ю з керівником департаменту на фоні його робочого місця. При збільшенні фото можна побачити пароль для входу у систему, що записаний на стікері та прикріплений до монітору.

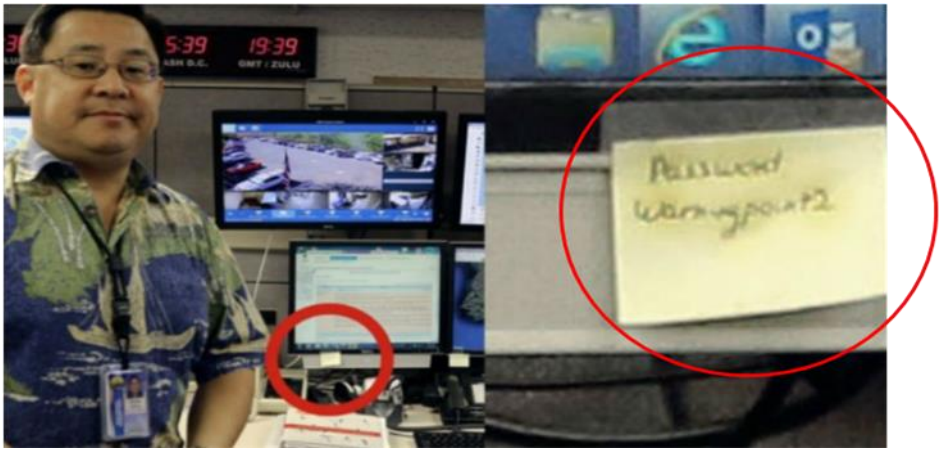


Фото з паролями прикріпленими до монітора у гавайській службі з надзвичайних ситуацій

Для зламу паролів використовують спеціальні програми

Чим складніший пароль був придуманий, тим складніше буде зловмисникам його підібрати. І мова йде як про комп'ютерні ресурси, так і про часові. Чим пароль довший, і використовує різні цифри, символ, спеціальні клавіші, тим більше часу знадобиться на підбір такого паролю.

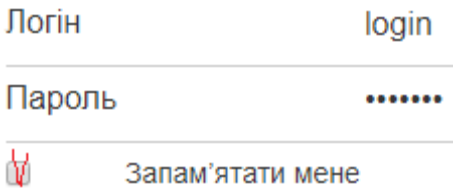
Існуючі програми для підбору паролів зазвичай працюють на основі двох підходів:

- база вже існуючих паролів – в цьому випадку програма перебирає всі можливі варіанти, що записані у її базі. Якщо такий пароль не відомий, то і підібрати його таким методом не можливо, але всі відомі і розповсюджені паролі, в тому числі на основі персональних даних тут підбираються дуже швидко.
- метод грубої сили (brute force) – більш складний, адже виконує перебір всіх можливих варіантів написання символів у паролю, поки не знайде правильну комбінацію, але при цьому його робота вимагає набагато більше часу та ресурсів, хоча врешті решт, потрібний пароль буде знайдений (може і через кілька років, а може за кілька секунд).

Password: T&p/E$v-O6,1@}
Время: 11 секунд! Чуток пришлось подождать.

Паролі можуть зберігатись на комп'ютері\телефоні

Тоді зловмиснику не треба підбирати паролів, оскільки вони можуть зберігатися для подальшого зручного входу в систему.



Вигляд форми із можливістю запам'ятовування логіну і паролю

Далі необхідно просто запустити програму для відновлення паролів і вуаля. До речі, дуже гарний спосіб як забути власний пароль.

Є спеціалізовані програмні та апаратні пристрої, що дозволяють обходити будь-яку схему перевірки входу в систему і, незалежно від паролів, отримувати доступ до даних

Ці засоби часто коштують достатньо велику кількість грошей (хоча і зустрічаються безкоштовні), але всі вони однозначно відносяться до заборонених, і можуть використовуватись лише уповноваженими органами. Від таких засобів може допомогти лише шифрування всіх даних на дисках.

Відбиток пальця може стати паролем

В цьому є велика перевага, користувачам не треба пам'ятати пароль, змінювати його. Здається, світ переходить на біометричні систем, що використовують вхід в систему за:

- відбитками пальців;
- сітківкою ока;
- геометричними параметрами обличчя;
- голосом;
- клавіатурним почерком тощо.

В цю індустрію вкладаються величезні кошти, багато виробників взагалі прогнозують відмову від звичайних паролів. І на фоні всіх захоплених відгуків, забувають про існуючі недоліки біометричних систем, що значно звужують їх використання.

Біометричний пароль теж можна підробити.

Коли мова заходить про біометричні паролі, всі якось забувають, наскільки просто скопіювати, а потім і підробити відбитки пальців. З сітківкою ока це зробити складніше, але теж не має нічого неможливого. Ще більш

складними є системи, що використовують динамічні біометричні зразки (наприклад клавіатурний почерк), але так само вони складні і в реалізації і використанні.

Але навіть не те, що підробити біометричні зразки легко є основною проблемою, а те, що їх в нас мало.

Скільки варіацій паролів можна придумати? А скільки у нас пальців? Уявіть собі ситуацію, коли зламали вашу електронну пошту: можна відновити контроль над нею (створити нову) і згенерувати новий пароль, якій зловмисник не буде знати. А що робити, якщо паролем є відбиток пальця? Використати інший? І скільки разів?

Використання біометричних паролів – це теж саме, що використання дуже складного символьного паролю, з усіма тими ж проблемами, але фактично без можливості зміни в разі компрометації.

Злам біометричних паролів потребує набагато менше часу

Сучасні програмні і апаратні засоби дозволяють взламати більшість символьних паролів, але вони вимагають достатньо велику кількість ресурсів. На взлам паролю до iPhone терориста із США ФБР витратило майже 1 млн. доларів і близько року на судові позови проти Apple.

В той час як на прикладання пальця до біометричного сканеру знадобиться лише кілька секунд. Ну а про легкість підробки відбитків пальців вже було сказано.

ПРОТИДІЯ

Використовуйте стійкий пароль:

- містить великі та малі літери;
- містить цифри і символи;
- більше 8 символів довжиною;
- не є словом ні на одній з мов, діалектів, жаргонів, сленгу;
- не ґрунтується на персональної інформації;
- не збережено в паперовій або електронній формі.

Періодично змінюйте паролі – раз на місяць/квартал, у випадку загрози кібератаки. Якщо ви підозрюєте, що ваш пароль став відомий комусь - змініть його негайно! Якщо ви підозрюєте, що ваш пароль став відомий комусь – негайно змініть його.

Не повідомляйте пароль в телефонних розмовах, е-поштою, в електронних опитуваннях, незнайомих формах авторизації тощо.

Нікому не повідомляйте пароль ні керівництву, адміністратору, технічній підтримці ні членам сім'ї та родичам.

Не повідомляйте принципи створення пароля («на основі прізвища», «моя собачка» , «українське слово латинськими літерами»).

Не використовуйте один пароль для різних систем (робочий обліковий запис, інтернет-банкінг, домашній інтернет-провайдер, електронна пошта, форуми).

Не записуйте паролі на папір чи файл, чи флешку.

РЕКОМЕНДАЦІЇ ЩОДО ГЕНЕРУВАННЯ ПАРОЛІВ

Розбийте всі паролі на кілька категорій

Перша категорія – загальнодоступні паролі для одноразових реєстрацій, електронних форм у магазинах тощо, там апріорі системи не є довіреними.

Оскільки все одно ці системи, скоріш за все, не використовують механізми захисту, і пароль може стати відомий шахраям, то використовуйте простий пароль з Топ10 паролів. Або придумайте простенький пароль типу 123qwe!@# і використовуйте на всіх подібних ресурсах.

Друга категорія – персональні паролі, які використовуються, наприклад, для інтернет-бакінгу, домашньої електронної пошти, соціальної мережі. Ці паролі необхідно змінювати десь раз на квартал (якщо у вас параноя, змінюйте частіше), і, зазвичай, вони можуть зацікавити досить багатьох.

Для генерації скористайтесь таким алгоритмом, **чим більше фантазії, тим краще**:

1. Оберіть базу паролю – наприклад, сьогодні середа – sereda.
2. Зробіть в базі заміни літер на цифри та символи – літеру s можна замінити на символ $, а літеру d на цифру 9. Другу літеру з великої і отримаємо

   $Ere9a
3. Для різних систем необхідно використовувати різні паролі, а отже на початок, в кінець або навіть у середину записуємо назву системи, наприклад пошта ukr.net, українською скоротимо до укр, на англійській розкладці – erh. Додаємо і отримуємо

   $Ere9a-erh
4. При необхідності замінювати раз на квартал додаємо ще відлік часу, наприклад перший трансформується у пер, трансліт per, отримаємо

   $Ere9a-erh-per

   Отримали складний пароль, що можна легко змінювати і налаштовувати під різні системи і час.

Третя категорія – робочі паролі, які використовуються, в системах, де є адміністратор, що іноді не за правилами вимагає повідомляти йому пароль, або має засоби, щоб його прочитати.

В такому випадку краще скористатися методом нав'язливих фраз. Наприклад,

Мені тринадцятий минало я пас ягнята за селом

або

До відпустки залишилось лише 10 місяців!!!

Трансформується за першими літерами у

М13мяпязс

або

Двзл10м!!!

Але не забуваємо про англійську розкладку клавіатури.

V13vzgzpc

або

Ldpk10v!!!

Відповідає всім вимогам і легко запам'ятовується, може змінюватись раз на місяць, причому з радістю.