ISSN 2078-6115. Вісник Львівського університету. Серія економічна. 2019. Випуск 56. С. 103-111
Visnyk of the Lviv University. Series Economics. 2019. Issue 56. P. 103-111

УДК 004:393.436:327.88 DOI: http://dx.doi.org/10.30970/ves.2019.56.0.3011

BIG DATA-ТЕХНОЛОГІЇ ТА ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

В. Приймак[1], Ю. Лєдяновський [2]

[1] Львівський національний університет імені Івана Франка
79008 м. Львів, проспект Свободи, 18
E-mail: pryimak_vasyl@ukr.net; vasyl.pryimak@lnu.edu.ua

[2]Академія сухопутних військ ім. Ген. Т. Костюшки
Республіка Польща, 51-147 Вроцлав, вул. Чайковського, 109
E-mail: jozef.ledzianowski@awl.edu.pl

Розглянуто особливості використання Big Data-технологій для обробки інформації в сучасних умовах розвитку IT-індустрії. Висвітлено проблеми, пов'язані з інформаційною безпекою України в цій ситуації. Наголошено на вкрай обмежених можливостях України щодо захисту персональних даних своїх громадян. Запропоновано заходи поліпшення інформаційної безпеки країни в нинішній ситуації.
Ключові слова: *Big Data-технології, великі дані, інформаційна безпека України, соціальні мережі, оператори мобільного зв'язку.*

Постановка проблеми. Швидкий розвиток інформаційно-комунікаційних технологій та широке використання їх у господарській діяльності і суспільному житті людини привів до лавиноподібного росту інформації, яку продукує населення планети. За оцінками експертів, інформаційний простір людства за одну хвилину збільшується набагато більше за його загальні обсяги до 2000 р. Тільки нещодавно набули широкого поширення такі терміни як «великі дані», «хмарні технології», «інтернет речей» та ін. Людство переосмислює розуміння світу і нашого місця в ньому.

Соціальні мережі, смартфони, безготівкові розрахунки, інтернет-покупки та інші способи продукування нової інформації привели до неможливості її обробки традиційними методами. Для обробки і аналізу великих даних було розроблено, так звані, Big Data-технології, оскільки традиційні інформаційні технології не могли справитись з такими великими обсягами інформації.

Перехід до нових методів і технологій обробки великих даних породив нові проблеми з захистом інформації, а в загальному – з інформаційною безпекою в країні. Захист великих даних і інформаційна безпека в Україні повинні бути організовані на більш високому рівні, для чого можна використати, зокрема, і Big Data-технології. Як показує огляд літературних джерел, дані проблеми ще мало вивчені науковцями нашої країни. Тому наукові дослідження цих проблем є актуальними і на часі. Вони особливо актуальні в сьогоднішніх умовах російської інформаційної війни проти України і необхідності захисту її інформаційного простору не тільки від країни-агресора, а й від деяких інших країн.

Аналіз останніх досліджень і публікацій. Дослідженню проблеми інформаційної безпеки України в умовах сучасної російської агресії, зокрема в умовах впровадження Big Data-технологій, присвятили свої наукові праці такі вчені: Т. Александрович, Г. Аніловська, В. Горбулін, М. Гуцалюк, Д. Дарчевська, А. Лелонек, В. Ліпкан, Я. Малик, Ф. Медвідь, В. Панченко, В. Світлична і деякі інші. Так, у наукових працях [1-3] висвітлено проблеми і загрози інформаційній безпеці України, способи зменшення їхнього впливу та можливості подолання, а в [4] обґрунтовано необхідність удосконалення національної політики України та Польщі по захисту їх від загроз і ризиків у інформаційній сфері, запропоновано рекомендації щодо цього удосконалення. Особливості захисту саме великих даних розглянуто в роботі [5], а проблеми забезпечення інформаційної безпеки та загрози національній і кібернетичній безпеці в умовах впровадження Big Data-технологій – в [6-8]. Водночас, в літературних джерелах недостатньо висвітлено проблеми інформаційної безпеки України обумовлені поширенням Big Data-технологій в суспільне життя і виробничу діяльність українців.

Метою даної роботи є дослідження стану і загроз інформаційній безпеці України в умовах впровадження Big Data-технологій та розроблення пропозицій щодо поліпшення стану цієї безпеки і протидії її загрозам.

Виклад основного матеріалу. Сьогодні, в процесі розвитку суспільства, обсяги генерованих в ньому даних ростуть з катастрофічною швидкістю. За прогнозами аналітиків, людство до 2020 р. випродукує більше 40 зеттабайт інформації, а за наступні п’ять років така інформація ще збільшиться в 10 разів. Інформаційні технології, які донедавна використовувались для обробки і аналізу інформації вже не можуть справлятись з такими великими потоками даних. Це зумовило розробку нових інформаційних технологій, які отримали назву Big Data-технології.

Термін Big Data започаткував Кліффорд Лінч у своїй статті про розвиток технологій обробки великих даних у 2008 р., а перші програмні продукти для роботи з великими масивами інформацій і мінімізації ризиків у процесі цієї роботи появились у 2010 р. В наступному році цією проблемою зацікавились великі IT-компанії і досить ефективно почали виробляти і впроваджувати в практику технології роботи з великими даними.

Слід зауважити, що установленого розуміння терміну Big Data в літературі немає. Одні автори під цим терміном розуміють саме великі дані, які мають певні характеристики, а засоби обробки цих даних називають Big Data-технології, інші – і великі дані і технології їх обробки називають одним терміном – Big Data. Ми будемо розрізняти ці поняття, тобто притримуватись першої точки зору.

В нашому розумінні Big Data це набір даних великих обсягів, які можуть бути неструктуровані, надходити для обробки в реальному часі і від багатьох джерел. Для роботи з ними потрібні спеціальні технології (будемо їх називати Big Data-технології), які відмінні від тих, що традиційно використовувались в IT індустрії для обробки даних. Big Data-технології задовольняють таким п’яти головним умовам ("п'ять V" умов):

- volume (обсяг) – обсяг нагромаджених даних, які дають змогу обробляти ці технології настільки великий, що його практично неможливо зберігати, обробляти та аналізувати традиційними способами. Для цього необхідно використати зовсім інший підхід та нові інструменти;

- velocity (швидкість) – швидкість нагромадження, обробки і аналізу даних постійно збільшується. Виникає потреба виконувати ці процедури в режимі реального часу, що можливо з використанням цих технологій;

- variety (різноманітність) – вказані технології дають можливість одночасно обробляти не тільки структуровану, а й неструктуровану інформацію, тобто таку, яку не можна класифікувати (привести до певної структури). Прикладом структурованої інформації можуть бути дані файлу про працівників підприємства (табельний номер, прізвище і ініціали, посада і інші характеристики), а неструктурованої – певний текст, фотографії чи відео з соціальних мереж;

- veracity (достовірність) – через бажання раціонального використання пам'яті для зберігання вхідної інформації, обсяги якої постійно збільшуються, виникає потреба у відокремленні корисної інформації від сміття. Тому система Big Data-технологій має підсистему фільтрації, яка розділяє інформацію цих двох категорій;

- variability (мінливість) – вхідна інформація не завжди чітко відображає стан чи тенденції розвитку досліджуваного об'єкта, що ускладнює обробку даних і вироблення висновків. У зв'язку з цим Big Data-технології мають засоби, які дають змогу оминути нетипову інформацію і виявити основні напрями розвитку цього об'єкта.

Таким чином, Big Data-технології – це набір інструментів і методів для нагромадження, обробки і аналізу структурованих, слабо структурованих і неструктурованих даних великих (більше 100 Гбайт) обсягів. Особливістю вказаних процедур є їх безперервність. Якщо традиційні методи обробки даних потребують структуризації даних і зберігання їх всіх на відповідному носії, то Big Data-технології дають змогу обробляти і аналізувати дані великих обсягів у реальному часі, ці дані можуть відрізнятися значною різноманітністю і швидкістю їх надходження. Висновки і рекомендації для прийняття рішень ґрунтуються, зазвичай, не на аналізі 100% опрацьованих даних, а не більше як на 10 їх відсотках. Хоча чим більше інформації для виконання аналізу і прогнозування використовують Big Data-технології, тим точніші результати вказаних процедур матимемо, тим досконаліше рішення з використанням результатів цих розрахунків буде прийняте.

Теоретичною основою Big Data-технологій є розділ інформатики, який називається «наука про дані». Він включає в себе наступне [9]:

- розроблення методології розподілених файлових систем і перетворення масивів даних шляхом використання методології відображення і згортки в якості інструментарію створення процедур паралельного і розподіленого оброблення надвеликих масивів даних;

- пошук за подібністю, включаючи ключові технології мінхешування (пошук перетинів в підмножинах масиву) і локально-чутливого хешування;

- обробка потокових даних і спеціалізовані алгоритми для даних, які швидко поступають і які повинні бути або негайно оброблені, або безповоротно втрачені;

- технології пошуку в надвеликих масивах даних і ранжування результатів пошуку (типу Google's PageRank);

- виявлення часто повторюваних підмножин даних, включаючи асоціативний пошук, метод «ринкових кошиків» і їх поліпшення;

- алгоритми кластеризації надвеликих масивів високої розмірності;

- проблеми веб-додатків: пошук адресатів для ефективного розсилання інформації та прогнозування переваг користувачів на основі вивчення їх активності в Інтернеті;

- алгоритми аналізу і вилучення структури дуже великих графів, зокрема графів соціальних мереж;

- методи отримання якісних і кількісних характеристик великих масивів даних шляхом зниження (редукції) розмірності, включаючи декомпозицію до єдиної величини, латентну (приховану) семантичну індексацію і різні види кореляцій;

- алгоритми машинного навчання, які можуть бути застосовані до великих даних.

Поява великих даних призвела не тільки до необхідності розроблення нових технологій їх оброблення і аналізу. Постало також питання безпеки цих даних. Разом з забезпеченням обчислювальної безпеки, постало питання захисту даних, які зберігаються і обробляються. Традиційним засобам захисту даних від їх викрадення, спотворення і знищення стало проблематично виконувати свої функції. Деякі з них, які можливо використати для захисту великих даних, надто загальмовують процес їхньої обробки. Також появились нові загрози і ризики. Разом з цими даними захищати потрібно використовувані для їх обробки програмні продукти. Бізнес потребує доступу до даних протягом круглої доби. У зв'язку з постійним ростом обсягів використовуваних даних не завжди вистачає місця для їх збереження. Становлення інтернету речей, і розширення соціальних мереж, повсюдне використання мобільних засобів зв'язку і інших пристроїв продукування великих даних привело до того, що під прицілом зловмисників опинилися всі моменти громадського життя. Тобто, інформаційна безпека особи, суспільства і держави стає однією з головних проблем в сучасному світі.

На відміну від раніше здійснюваних компаніями дій з управлінням майном, грошима та інтелектуальною власністю, сьогодні з'явився новий актив – дані, які не лише використовуються для прийняття управлінських рішень, але і самі стали товаром [12]. Сьогодні джерелами даних стали смартфони, ноутбуки, квитанції супермаркетів, соціальні мережі, інтернет-покупки, банкомати, смарттелевізори тощо, які надають деталізовану інформацію про погляди та поведінку їх власників. Тисячі елементів такої «інформаційної мозаїки» щоденно збираються в єдиний профіль користувача, «віртуальну» скриньку із пов'язаних між собою баз даних, який може використовуватися без відома їх власника для отримання прибутку третіми особами [7]. Тому потрібно розробляти технології, які б унеможливили такі дій і захистили власні дані користувачів цих технічних засобів від використання сторонніми особами.

Слід зауважити, що у порівнянні з традиційними проблемами інформаційної безпеки (конфіденційність, цілісність і доступність інформації) проблеми безпеки великих даних характеризуються певними особливостями. До них можна віднести: «відсутність досвіду щодо захисту Big Data, а відтак і відсутність підготовлених фахівців для вирішення таких завдань; відсутність методології та стандартів захисту Big Data; велика, неоднорідна, динамічно зростаюча структура Big Data; відсутність правового регулювання Big Data; при використанні великої кількості даних зростає ймовірність їх витоку; Big Data стають джерелом для APT-атак (advanced persistent threat — «розвинута стійка загроза, або таргетована кібератака, що спрямована на конкретного об'єкта, може тривалий час здійснюватися приховано у різних напрямках та ґрунтується на зібраних про об'єкт даних, у тому числі шляхом соціальної інженерії)» [8].

Для України в нинішніх умовах неоголошеної російської війни проблема інформаційна безпека особливо актуальна. Анексії Криму і війні на Донбасі

передували потужні інформаційні атаки Кремля на населення як цих територій, так і всієї країни, які не припиняються і сьогодні. Робота значної частини складу інформаційних військ, які створені в сусідній державі, спрямована на нашу країну. Це можна підтвердити багатьма фактами. Для прикладу можна взяти останні вибори президента України. Аналіз вмісту інформаційних повідомлень українських громадян і відповідні заходи на основі зроблених узагальнень, спеціальна реклама в інтернеті, сотні і навіть тисячі ботів, «фейкові» групи в соціальних мережах та інші дії цих військ, які були спрямовані на компрометацію діючого тоді Президента України, дали свій результат. Під впливом цієї пропаганди, яка лилася на виборців з усіх інформаційних джерел, велика частина з них голосувала не так за Зеленського, як проти Порошенка.

Відповідні російські служби можуть безперешкодно слідкувати за пересуванням українських громадян, а також отримувати їх особисту інформацію і персональні дані. Причому для виконання цієї роботи, до моменту блокування доступу до російських сервісів «Одноклассники», «Вконтакті», «Яндекс» чи «Мейл.Ру», працівникам відповідних російських відомств застосовувати великі зусилля не потрібно було, нічого не треба було зламувати. Досить було комусь з них звернутись у офіс потрібного сервісу. Це підтверджують такі слова керівника «Вконтакті» у листі до Суркова: «Як Ви знаєте, ми вже декілька років співпрацюємо з ФСБ і відділом «К» МВС, оперативно видаючи інформацію про тисячі користувачів нашої мережі у виді IP-адрес, номерів мобільних телефонів і іншої інформації, яка необхідна для їх ідентифікації» [10]. Тобто, заборона цих сервісів стала позитивним кроком у зміцненні інформаційної безпеки України.

Однак, після накладення санкцій на «Mail.Ru Group» і заборони цих сервісів ситуація в сфері захисту інформаційного поля України не надто змінилась. Адже залишився в нашій країні підконтрольний Кремлю мобільний зв'язок, російські інформаційні війська можуть використовувати і використовують для маніпулювання громадською думкою населення України та розпалювання ворожнечі між її громадянами інші соціальні мережі.

Найкрупніші в Україні оператори мобільного зв’язку належать власникам, які різним чином пов’язані з російським капіталом. За оцінками експертів, російський капітал забезпечує 97% мобільного покриття в Україні. Зокрема, такі компанії як «Київстар» і «Лайф» через різні дочірні компанії та підставних осіб належать «Альфа-Груп», керівником і співвласником якої є російському олігарх українського походження М. Фрідман. Притому сьогоднішнім президентом компанії «Київстар» є росіянин Чернишов П. А., який у 2015 р. отримав українське громадянство. Що стосується «Vodafone», то це бренд, який надала згідно офіційного договору російській компанії «МТС» британська компанія з такою ж назвою. Кінцевим власником «МТС» є росіянин Євтушенко Володимир Петрович [10].

Оператори, які забезпечують мобільний зв’язок на території України запускають власні месенджери з безплатними повідомленнями, дзвінками і новинами, завдяки яким можуть безперешкодно зчитувати персональні дані у своїх користувачів. Зокрема, материнський холдинг «Київстар» Veon ще літом 2017 р. повідомив про запуск нового додатка, в якому трафік для абонентів мережі не буде тарифікуватись і абонент зможуть користуватися ним навіть при нульовому рахунку [11]. Для залучення нових клієнтів постійно відбувається розширення платформи, надаються нові можливості, які пов’язані з використанням мобільного інтернету, підключенням партнерів тощо.

Крім інформації мобільних операторів, російські спецслужби і інформаційні війська для своєї підривної роботи в Україні широко використовую ті соціальні мережі, які в нас не заборонені. Такі дій Кремль практикує не тільки по відношенню до України, але й до багатьох інших країн, зокрема, до Сполучених Штатів Америки. На це вказують світові засоби масової інформації.

При розгляді комітетом з розвідки американського сенату питання використання Росією соціальних мереж при втручанні її у президентські вибори США 2016 року Google, Facebook і Twitter визнали, що стали інструментом для маніпуляцій Росії. Керівники останнього навіть пообіцяли реабілітуватися, віддавши зароблені на російських кампаніях гроші на просування демократії. У кожній з компаній пообіцяли або зробити рекламу прозорішою, або ретельніше працювати над безпекою. В процесі розгляду цього питання сенатори зауважили, що на схожі маніпуляції перед виборами президента Америки Росія витратила 300 тисяч доларів [12]. Тобто розглянуте питання стосується як інформаційної, так і національної безпеки країн, які піддаються російським інформаційним атакам. Для захисту інформаційного простору України суттєвим є те, що головні офіси найбільших у світі соціальних мереж розміщені також не на її території. Українські інформаційні служби не мають можливості впливати на дії цих ІТ компаній і впроваджувати свою політику інформаційної безпеки держави.

В умовах динамічного розвитку Big Data-технологій розпорядниками персональних даних українських громадян через соціальні мережі є американські компанії, а даних мобільних сервісів – підконтрольні російській владі оператори зв'язку. На сьогодні, Україна має вкрай обмежені можливості щодо захисту персональних даних своїх громадян, що врешті може призвести до втрати ще однієї складової суверенітету нашої держави [8].

В сучасних умовах розвитку інформаційних технологій і необхідності захисту великих даних Росія продовжує розробляти нові засоби контролю інформаційного простору інших країн, приймає законодавчі акти, які зобов'язують операторів зв'язку зберігати відомості про факти комунікації абонентів (аудіозаписи дзвінків, переписку, зображення, відео тощо), а іноземні ІТ-компанії – зберігати персональні дані росіян на серверах, що знаходяться в межах РФ, прагне стати лідером у сфері штучного інтелекту, у сферу якого протягом 10 останніх років вклала близько 23 млрд руб державних інвестицій [7]. Це сьогодні повинна ураховувати Україна при реалізації своєї стратегії інформаційної безпеки.

Розглядаючи висвітлену проблему інформаційної безпеки в епоху Big Data, слід звернути увагу на два основних її аспекти. Перший аспект полягає у безпеці самих великих даних. Тут необхідно чітко ідентифікувати та класифікувати дані і джерела, які їх продукують, опрацьовують і аналізують, зберігають і передають. Порядок тільки допоможе контролювати набори великих даних, сприятиме їхній інформаційній безпеці.

Другий аспект полягає у дослідженні можливості поліпшення інформаційної безпеки великих даних за рахунок використання їх аналітики і впровадження сучасних Big Data-технологій. Наприклад, результати аналізу великих даних, потоків їх поступлення на обробку можна використати для машинного навчання чи проектування моделей прогнозування, за допомогою яких визначити моменти можливої небезпеки і її джерела.

Ураховуючи сказане, потрібна нова національна програма інформаційної безпеки України в сучасних умовах великих даних, яка б ураховувала можливість

використання для їх захисту Big Data-технології. Треба розповсюджувати серед населення відомості про походження капіталу операторів мобільного зв'язку і власників соціальних мереж, інформувати громадян країни про можливість використання сторонніми особами поширеної в соціальних мережах чи за допомогою мобільного зв'язку інформації на шкоду її власникам, повідомляти українців про способи захисту своїх даних. Окрема увага державних органів повинна бути зосереджена на інформуванні бізнесменів. Національно свідомі підприємці мають розуміти ситуацію з інформаційною безпекою в країні і, при можливості, сприяти захисту інформаційного простору держави за допомогою капітальних вкладень у розвиток українського мобільного зв'язку і власних соціальних мереж.

Українські громадяни повинні постійно пам'ятати про те, що опублікована ними в інтернеті інформація може бути використана проти них. Особливу увагу треба звертати на додатки і до якої інформації вони мають доступ, оскільки збір даних найчастіше відбувається через додатки чи тести. Потрібно також знати, що вся інформація, яку отримали від вас друзі, можуть отримати й інші користувачі.

Висновки. Виконані дослідження показали, що з появою великих даних при реалізації національної безпеки України особливу увагу потрібно звертати на її інформаційну безпеку, оскільки майже всі мобільні оператори належать підконтрольним російській владі власникам, а розпорядниками даних в соціальних мережах є американські компанії. В цих умовах треба розробити національну програму інформаційної безпеки України, яка б ураховувала можливість використання для їх захисту Big Data-технології, впровадити інші запропоновані вище заходи інформаційної безпеки країни.

---

1. Гуцалюк М.О. Інформаційна безпека України: нові загрози / М.О. Гуцалюк // Бизнес и безопасность. – 2007. – № 5. – С. 2–3.
2. Світлична В.Ю. Інформаційна безпека: Сутність та порядок реалізації / В.Ю. Світлична // «Молодий вчений». – 2014. – № 11 (14). – С. 97-100.
3. Медвідь Ф. Інформаційна безпека України: виклики та загрози / Ф. Медвідь // URL : http://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf (дата звернення: 30.07.2019).
4. Приймак В. Інформаційна безпека України та Польщі в умовах російської інформаційної війни // В. Приймак, М. Луцик / Współpraca Europejska. – 2017. – Nr. 10 (29). – S. 9-20.
5. Маслова Н.О. Особливості захисту даних великих обсягів / Н.О. Маслова, М.А. Федорко // Наукові праці ДонНТУ, Серія «Інформатика, кібернетика та обчислювальна техніка». – 2018. – № 1 (26). – С. 41-46.
6. Фактор информационной безопасности в процессе эволюции гетерофазных мультиагентных когнитивных систем [Електронний ресурс] / А.У. Заммоев, Ю.Х. Хамуков, Л.З. Шауцукова // Режим доступу: https://www.science-education.ru/pdf/2014/6/727.pdf .
7. Панченко В.М. Загрози національній безпеці України в умовах впровадження BigData-технологій / В.М.Панченко // Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. – С. 127-131.
8. Панченко В.М. BigData-технології як загроза кібернетичній безпеці держави / В.М.Панченко // Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 26 квітня 2018 р. / Маріупольський

державний університет; уклад. Проценко О.Б., Меркулова К.В. – Маріуполь: МДУ, 2018. – 145 с.
9. Rajaraman A. Mining of Massive Datasets / Rajaraman A., Leskovec J., Ullman J. D. – Cambridge University Press, 2011. – 326 p.
10. Мобильные операторы Украины или кого могут слушать спецслужбы РФ [Електронний ресурс] / Дмитрий Мацкевич // Режим доступу: https://stopterror.in.ua/info/2017/06/mobilnye-operatory-ukrainy-ili-kogo-mogut-slushat-spetssluzhby-rf/.
11. Владелец «Киевстар» запускает в Украине мессенджер с бесплатными сообщениями, звонками и новостями [Електронний ресурс] / Павел Красномовец // Режим доступу: https://ain.ua/2017/07/19/veon-kyivstar-prilozheniye/.
12. «Троянський кінь» Кремля: соцмережі визнали, що їх використали для маніпуляцій у США [Електронний ресурс] / Остап Яриш, Наталія Гуменюк // Режим доступу: https://hromadske.ua/posts/rosiya-cherez-socmerezhi-manipulyue-amerikancyami.

References

1. Hutsaliuk M.O. (2007). Informatsiina bezpeka Ukrainy: novi zahrozy, *Byznes y bezopasnost,* 5, pp.2–3.
2. Svitlychna V.Iu. (2014). Informatsiina bezpeka: Sutnist ta poriadok realizatsii, *«Molodyi vchenyi»,*11 (14), pp. 97-100.
3. Medvid F. Informatsiina bezpeka Ukrainy: vyklyky ta zahrozy, URL : http://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf (data zvernennia: 30.07.2019).
4. Pryimak V. (2017). Informatsiina bezpeka Ukrainy ta Polshchi v umovakh rosiiskoi informatsiinoi viiny, *Współpraca Europejska,*10 (29), pp.9-20.
5. Maslova N.O. (2018). Osoblyvosti zakhystu danykh velykykh obsiahiv, *Naukovi pratsi DonNTU*, *Seriia* «*Informatyka, kibernetyka ta obchysliuvalna tekhnika*», 1 (26), pp.41-46.
6. Zammoev A.U.,. Khamukov Yu.Kh, Shautsukova L.Z. Faktor ynformatsyonnoi bezopasnosty v protsesse эvoliutsyy heterofaznыkh multyahentnыkh kohnytyvnыkh system, URL: https://www.science-education.ru/pdf/2014/6/727.pdf .
7. Panchenko V.M. (2018). Zahrozy natsionalnii bezpetsi Ukrainy v umovakh vprovadzhennia BigData-tekhnolohii, *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy : zb. tez nauk. dop. nauk.-prakt. konf.* (Kyiv, 30 bereznia 2018 r.) [Elektronne vydannia], Kyiv : Nats. akad., SBU, pp.127-131.
8. Panchenko V.M. (2018). BigData-tekhnolohii yak zahroza kibernetychnii bezpetsi derzhavy, *Kiberbezpeka u systemi natsionalnoi bezpeky Ukrainy: priorytetni napriamy rozvytku: zbirnyk materialiv naukovoho kruhloho stolu*, m. Mariupol, 26 kvitnia 2018 r. / Mariupolskyi derzhavnyi universytet; uklad.
9. Rajaraman A. (2011). Mining of Massive Datasets, Cambridge University Press, 326.
10. Mobilnye operatory Ukrainy ili koho mohut slushat spetssluzhby RF, URL: https://stopterror.in.ua/info/2017/06/mobilnye-operatory-ukrainy-ili-kogo-mogut-slushat-spetssluzhby-rf/.
11. Vladelets «Kyevstar» zapuskaet v Ukrayne messendzher s besplatnymi soobshchenyiamy, zvonkamy y novostiamy, URL: https://ain.ua/2017/07/19/veon-kyivstar-prilozheniye/.
12. Yarysh O, Humeniuk N. «Troianskyi kin» Kremlia: sotsmerezhi vyznaly, shcho yikh vykorystaly dlia manipuliatsii u SShA, URL: https://hromadske.ua/posts/rosiya-cherez-socmerezhi-manipulyue-amerikancyami.

BIG DATA TECHNOLOGIES AND INFORMATION SECURITY OF UKRAINE

V. Pryimak[1], J. Ledzianowski[2]

1. Department of Information Systems in Management,
Ivan Franko National University of Lviv
Prospect Svobody 18, Lviv, UKRAINE

2. Department of Management, The General Tadeusz Kosciuszko Military Academy of Land Force, Chaikonskogo st., 109, Wroclaw, POLAND

The article discusses the peculiarities of information processing in the modern conditions of IT industry development. In the development process of modern society, it is noted the catastrophic rate of growth of the volume of data generated in that society. This has led to the development of new information technologies, called Big Data technologies.

Is described the essence of the Big Data technologies, the history of its origin and the author's understanding of this concept, what are theoretical basis of those technologies and conditions, which they satisfy. It is stated that Big Data technologies are a set of tools and methods for accumulation, processing and analysis of structured, poorly structured and unstructured data of large (more than 100 GB) volumes. The peculiarity of these procedures is their continuity. Unlike traditional information-processing methods, which require data to be structured and stored on the appropriate media, Big Data technologies allow large amounts of data to be processed and analyzed in real-time. This data can differ greatly by the variety and speed of its receipt.

Highlighted the problems related to the protection of big data and general information security of Ukraine under the current conditions of information technologies development and distribution of large amounts of information. Based on the analysis of national identity of the owners of mobile network operators and managers of data in social networks in Ukraine, it is concluded that the largest mobile operators in Ukraine belong to owners who are differently connected with Russian capital, and are American companies are the managers of personal data of Ukrainian citizens through social networks. Ukraine has very limited capacity to protect the personal data of its citizens. Although it is possible to use developed Big Data technologies.

It is proposed the information policy ideas in the country, the implementation of which will improve the information security of the country in the current situation of using big data by society.

Keywords*:* Big Data technologies, big data, information security of Ukraine, social networks, mobile network operators