НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ
ИНСТИТУТ ПРОБЛЕМ РЕГИСТРАЦИИ ИНФОРМАЦИИ НАН УКРАИНЫ

НАЦИОНАЛЬНАЯ АКАДЕМИЯ ПРАВОВЫХ НАУК УКРАИНЫ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ИНФОРМАТИКИ И ПРАВА

НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ УКРАИНЫ «КПИ»
УЧЕБНО-НАУЧНЫЙ ЦЕНТР ИНФОРМАЦИОННОГО ПРАВА И ПРАВОВЫХ ВОПРОСОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ФСП

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

ВЫПУСК 15

Киев – 2015

Рекомендовано к печати ученым советом
Института проблем регистрации информации НАН Украины (протокол № 4 от 13 октября 2015 г.)

Информационные технологии и безопасность. Материалы международной научной конференции ИТБ-2015. – К.: ИПРИ НАН Украины, 2015. – 253 с. ISBN: 878-966-2344-34-9

В сборник вошли материалы, представленные на Международной конференции «Информационные технологии и безопасность» (ИТБ-2015, 21 октября 2015 года в г. Киев, Украина).

Сборник охватывает широкий круг актуальных проблем обеспечения информационной и кибербезопасности, противодействия информационной агресии и кибертерроризму, проведения информационно-аналитических исследований на основе контента в сети Интернет, правового обеспечения информационной безопасности.

ISBN 878-966-2344-34-9

АРХІТЕКТУРА СИСТЕМИ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Додонов О.Г., Ланде Д.В., Коваленко Т.В.
Інститут проблем реєстрації інформації НАН України

Створення автоматизованої системи інформаційної підтримки процесів протидії ворожим інформаційним компаніям, виконання заходів щодо відбиття деструктивних зовнішніх і внутрішніх інформаційних впливів – актуальна проблема сучасності, особливо в умовах ведення інформаційних війн [1], [2].

В якості основних завдань такої системи розглянемо:

- побудову сценаріїв протидії інформаційним деструктивним впливам на основі деякої онтології понять;
- контент-моніторинг (безперервний змістовний аналіз) інформаційного простору з урахуванням знань експертів;
- виявлення закономірностей (трендів) і аномалій шляхом аналізу динаміки зміни значень окремих факторів;
- виявлення інформаційних впливів та інформаційних операцій;
- прогнозування розвитку інформаційних сюжетів та ситуацій;
- оцінка ефективності процедур інформаційної підтримки прийняття рішень.

Відповідно, для реалізації такої системи інформаційної підтримки процесів, пов'язаних, зокрема, з національною безпекою необхідно:

- створити онтологію понять предметної області (вузлів – факторів безпеки і відповідних причинно-наслідкових (казуальних) зв'язків – залежностей факторів), визначити вид цільової функції безпеки об'єктів-вузлів цієї онтології залежно від значень факторів безпеки;
- постійно актуалізувати значення факторів безпеки і зв'язків залежно від результатів моніторингу інформаційного простору та знань експертів;
- визначати можливі сценарії на основі аналізу онтології і виявлення відповідних часткових онтологій;
- аналізувати динаміку зміни значень окремих факторів та зв'язків з метою виявлення закономірностей, прогнозування;
- постійно проводити оцінку ефективності проведеної інформаційної підтримки.

Для рішення цих завдань, передбачається, що система інформаційної підтримки повинна складатися з трьох основних підсистем (рис. 1): підсистеми введення онтології понять, підсистеми моніторингу

інформаційного простору, підсистеми аналітичної обробки, та відповідних інтерфейсів з адміністраторами і користувачами.

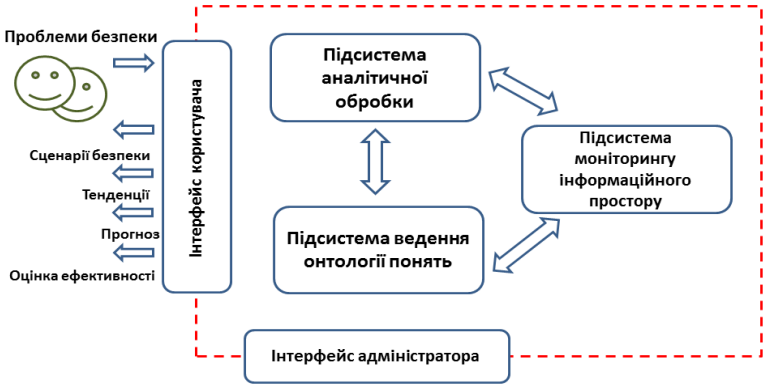


Рис. 1. Архітектура системи інформаційної підтримки

Онтології понять предметної області

Онтологія в даному випадку являє собою функціональний аналог бази знань, що відбиває знання експертів про предметної області, тобто в якості вузлів графа онтології вибираються найважливіші фактори предметної області забезпечення безпеки, а в якості зв'язків – причинно-наслідкові зв'язки між факторами (з математичної точки зору – граф з направленими ребрами) [3]. Вузлам і зв'язкам приписуються числові значення, які в подальшому можуть коригуватися. Зв'язки також можуть мати різну вагу (силу впливу) і бути як позитивними (збільшення значення першого фактора приводить до збільшення значення другого чинника), так і негативними (збільшення значення першого фактора приводить до зменшення значення другого чинника).

Визначення можливих сценаріїв на основі аналізу онтології

Сценарії інформаційної підтримки, як правило, зв'язуються з певними факторами безпеки (найчастіше об'єктами і уразливостями). Після вибору цільових факторів сценарію в графі онтології виявляються підграфи (часткові онтології), найтісніше пов'язані з вибраними чинниками. Далі вирішується завдання часткової оптимізації цільової функції на обраних підграфах, тобто обчислюється цільова функція в залежності від змін факторів безпеки, що відповідають можливим сценаріями.

Динаміка зміни значень окремих факторів і зв'язків

Аналіз динаміки зміни значень окремих факторів безпеки і зв'язків в часі (як по їхньому відображенню в інформаційному просторі, так і внесених експертами) дозволяє виявляти деякі закономірності зміни цих факторів (періодичності, тренди, аномалії) шляхом застосування сучасних засобів цифрової обробки сигналів (регресійний, дісперсійний, вейвлет-аналіз тощо), виявляти можливі інформаційні операції шляхом порівняння з відповідними шаблонами їх динаміки, а також здійснювати прогнозування [4].

Контент-моніторинг інформаційного простору

Сьогодні мережа Інтернет утворює значимий динамічний сегмент інформаційного простору, інформаційні потоки, зміст та обсяги яких необхідно враховувати при проведенні аналітичних досліджень. Основним об'єктом аналізу при цьому є подієві або тематичні зрізи цих потоків – масиви інформаційних повідомлень, документів, що відповідають певним подіям або тематикам.

Завдання підсистеми моніторингу інформаційного простору наступні:

- моніторинг цільових об'єктів;
- знаходження релевантних тематичних повідомлень в інформаційному просторі;
- контроль медіаприсутності і медіаактивністю цільових об'єктів;
- виявлення нових об'єктів моніторингу;
- формування ретроспективних фондів для подальшого аналізу.

Підсистема аналітичної обробки

Підсистема аналітичної обробки являє собою аналітичний блок системи інформаційної підтримки, що забезпечує вирішення наступних завдань:

- визначення динаміки тематичних сюжетів;
- визначення критичних точок в динаміці тематичних сюжетів;
- відстеження сюжетних ланцюжків, відповідних подій, процесів;
- виявлення основних подій і об'єктів з тематичного сюжету;
- виявлення і візуалізація взаємозв'язків подій і об'єктів моніторингу, а також об'єктів моніторингу між собою.

У відповідності зі своїм призначенням дана підсистема, разом з підсистемою моніторингу інформаційного простору, дозволяє реалізувати наступні етапи інформаційно-аналітичного дослідження [5]:

- формування запиту в середовищі обраної системи. Знаходження тематичних публікацій за запитом за допомогою систем контент-моніторингу;
- визначення динаміки тематичних публікацій за запитом;
- визначення критичних точок в динаміці тематичних публікацій;
- визначення основних подій у критичних точках;

- виявлення об'єктів моніторингу;
- виявлення та візуалізація взаємозв'язків;
- прогноз розвитку подій.

Висновки

У доповіді представлена архітектура системи інформаційної підтримки прийняття рішень, ідеологія створення та використання онтологій для побудови сюжетів інформаційної протидії, детально розглянуто методику аналітичного дослідження, яка базується на використанні інструментальних засобах аналізу і візуалізації інформаційних потоків і часових рядів.

Запропоновані архітектурні рішення можна використовувати при реалтізації систем інформаційної підтримки прийняття рішень, що базуються на контент-моніторингу інформаційного простору та сценарному аналізі, а так само в якості бази для проведення аналітичної та прогнозної діяльності.

Литература

1. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операции та безпека Суспільства: Загрози, протідія, моделювання: монографія. – К .: Інтертехнологія, 2009. – 164 с.

2. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Сценарный анализ эффективности управления информационной поддержкой государственной политики России в Арктике. // Национальная безопасность / nota bene. – 2011. – № 6. – С. 104-137.

3. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Структурно-динамический подход к сценарному анализу процессов информационного противоборства в Арктике // Труды XII Всероссийского совещания по проблемам управления (ВСПУ 2014). – М.: ИПУ РАН, 2014. – С. 8889-8901.

4. Додонов А.Г., Ландэ Д.В. Моделирование и анализ тематических информационных потоков // Информационное противодействие угрозам терроризма, 2013. – № 20. – С. 52-59.

5. Додонов А.Г., Ландэ Д.В. Методика аналитического исследования динамики событий на основе мониторинга веб-ресурсов сети Интернет // Информационные технологии и безопасность: основы обеспечения информационной безопасности: Материалы международной научной конференции ИТБ-2014. – К.: ИПРИ НАН Украины, 2014. – С. 3-17.

О ДЕЯКИХ ПРИНЦИПОВИХ МОМЕНТАХ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Фурашев В.М.
Науково-дослідний інститут інформатики і права НАПрН України

Широкомасштабна інформатизація, створення, впровадження їх у повсякденне життя людини, суспільства і управління на всіх рівнях та стрімкий їх розвиток викликало певні, причому досить суттєві, зміни суспільних відносин. Зміни відбуваються як на формальному, так й неформальному, емоційно-психологічному, рівнях, що не може відобразитися на соціалізації людини. Держава, як єдине джерело правового регулювання суспільних відносин, повинно враховувати та адекватно реагувати на ці процеси. Розуміння, в першу чергу у загальному, а не приладному аспекті, сутності процесів, які відбуваються у інформаційної сфері, напряму впливає на стратегію і тактику розбудови, впровадження та зміцнення системи інформаційної безпеки.

У зв`язку з цим, до уваги та, сподіваємося, подальшу дискусію учасників Міжнародної конференції «Інформаційні технології та безпека» (ІТБ-2015, пропонується деякі визначення термінів, які досить широко застосовуються у інформаційної сфері та сфері інформаційної безпеки та які декілька відрізняються від законодавче прийнятих або вживаємих у науковій літературі. Метою пропонуємої дискусії є пошук найбільше точного відображення загальної (природної або штучної) сутності дії, процесу, явища до якого застосовується тій чи інший термін.

Безпека інформації – 1) стан інформації, якій визначається рівнем відповідності (ідентичності) першоджерелу інформації (оригіналу, копії) після здійснення з нею визначених дій (передачі-прийому, обробки та ін.); 2) склад та стан інформації, а також дії з нею, за яких забезпечується визначений рівень інформаційної безпеки.

Безпечність інформації **–** показник відповідності спрямованості та змісту інформації національним інтересам держави та суспільства у всіх сферах забезпечення життєдіяльності, суспільно прийнятим нормам і правилам відношень у морально-етичному та психологічному поводженні з інформацією, законодавчо визначеним вимогам до інформації.

Достовірність інформації **–** характеристика вірогідності інформації як міри тотожності інформації з першоджерелом або точність передачі інформації, віддзеркалення дійсності (істинного стану справ).

Загрози інформаційної безпеці **–** 1) обставини, події, дії (штучні або природні) які негативно впливають на стан і рівень інформаційної безпеки або перешкоджають їх зміцненню та підвищенню; 2) наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері.

Захист інформації – комплекс заходів, що проводяться з метою запобігання витоку, розкраданню, втраті, несанкціонованому знищенню, спотворенню, модифікації (підробки), несанкціонованому копіюванню, блокуванню інформації та несанкціонованому доступу до апаратури, програм і даних.

Інформаційна технологія – цілеспрямована організована сукупність дій та процедур забезпечення обороту інформації (створення, поширення (передачі), використання, зберігання та знищення (утилізації) інформації).

Кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Кіберпростір – форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на сприйняття, запам`ятовування, переробку та обмін інформацією.

Носій інформації – об`єкт/об`єкти матеріального та нематеріального світу, незалежно від форми та засобу їх утворення та існування, який/які має/мають властивості сприйматися/потенційно сприйматися хоча б одним з органів чуття живої істоти та викликати відповідне реагування, а також штучною системою, яка спроможна саморозвиватися (самонавчатися) або сприймати, через визначені пристрої, занесену на ці об`єкт/об`єкти інформацію.

З метою уникнення нав`язування особистої думки не наводиться аргументація викладених положень. Аргументацію залишаємо для дискусій.

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Авраменко М.С.
Київський Національний університет імені Т. Шевченка

Так звана «гібридна війна» на Донбасі постійно супроводжується інформаційно-психологічними атаками, ініційованими як терористами «ДНР» та «ЛНР», а також політичним керівництвом країни-агресора. Російські інформаційні операції для забезпечення інформаційної переваги в Україні набувають все нових форм, в залежності від особливостей розвитку військово-політичної обстановки. РФ використовує будь-який інформаційний привід, або штучно створену провокацію, щоб розпочати чергову антиукраїнську інформаційну атаку. Підтримка інформаційної експансії РФ здійснюється на всіх політичних рівнях (президент РФ, МЗС, політичні сили РФ, закордонні представництва РФ, у т.ч. – в ОБСЄ, ООН, інших міжнародних інституціях).

Спостерігаються тенденції щодо нарощування зусиль держави-агресора в напрямку розширення присутності в інформаційному просторі України з позицій представництв власних медіа-структур, або контрольованих ними вітчизняних мас-медіа, які діють у фарватері зовнішньополітичної спрямованості РФ та забезпечують інформаційну підтримку дій керівництва держави-агресора по відношенню України та її міжнародних інтересів.

Таким чином, існує високий рівень зовнішніх загроз інформаційній сфері України, викликаних інформаційно-пропагандистською експансією з боку РФ. Ведення РФ інформаційної війни одночасно з прямою військовою агресією є важливим елементом «гібридної» війни проти України. Здійснюються спроби через інформаційну сферу впливати на процеси в нашій державі з метою деморалізації суспільства та посилення протестних настроїв.

Для посилення інформаційної безпеки України та протидії зовнішньому негативному інформаційному впливу на свідомість населення, із використанням каналу журналістського обміну, доцільним в сучасних умовах є вирішення питання щодо повернення акредитації іноземних представників засобів масової інформації при МЗС України, за відповідністю, з вимогами країн їх місця роботи, у зв’язку з чим пропонується внести зміни до Закону України «Про інформацію» [1], зокрема ст. 26. «Акредитація журналістів, працівників засобів масової інформації» доповнити новим розділом «Акредитація іноземних журналістів», в якому визначити, що їхня акредитація здійснюється Міністерством закордонних справ України, у зв’язку з чим необхідним є розробка нового Положення «Про акредитацію в Україні іноземних кореспондентів та представників іноземних засобів масової інформації».

Також доцільно прискорити розробку та прийняття Стратегії розвитку інформаційного простору в Україні, Стратегії кібернетичної безпеки України з метою формування сприятливих умов для розбудови інформаційного суспільства, удосконалення системи державного управління на основі використання ІКТ; забезпечення відкритості інформації про діяльність органів державної влади й місцевого самоврядування, розширення доступу до неї та надання можливості безпосередньої участі людини та інститутів громадянського суспільства в процесах підготовки та експертизи проектів політико-адміністративних рішень, контролю за результативністю й ефективністю діяльності органів державної влади та органів місцевого самоврядування.

Тож розвиток України як правової демократичної держави неможливий без переходу й розвитку інформаційно відкритого суспільства, що передбачає виникнення нових форм інформаційної взаємодії державної влади із суспільством. Насамперед, державна влада має здійснювати відкриту і чесну інформаційну взаємодію з громадськістю через засоби масової комунікації [2, с.56].

В сучасних умовах, на виконання рішення Ради Національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [3], необхідним також є прискорення прийняття законопроекту «Про основні засади забезпечення кібербезпеки України», що дозволить визначити пріоритетні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, створити систему надійного захисту цілісності державних інформаційних ресурсів, визначити правові засади боротьби з кібертероризмом та кіберзлочинністю.

Концептуальні засади інформаційної безпеки мають формуватися, виходячи з національних інтересів країни, збалансовуючи інтереси особистості, суспільства і держави, а також з урахуванням проведення на Сході України антитерористичної операції.

Пріоритетними напрямками і завданнями національної системи забезпечення інформаційної безпеки держави повинні бути наступні:

- відкритість та інформованість суспільства про діяльність її органів і суспільних інститутів в інформаційній сфері;
- державна політика у сфері суспільних відносин повинна спрямовуватися на забезпечення права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційної діяльності в національному інформаційному просторі України;
- всебічна державна підтримка національних засобів масової інформації, забезпечення соціально-правового захисту професійних творчих працівників, які займаються інформаційною діяльністю; стимулювання вітчизняних фундаментальних та прикладних

досліджень, розробки у сфері інформатизації, телекомунікацій і зв'язку;
- розробка та схвалення, з метою уніфікації інформаційних відносин, «Інформаційного кодексу України»;
- посилення контролю за додержанням законодавства з питань кібернетичної безпеки;
- створення системи інформаційно-аналітичного забезпечення органів державної влади, прийняття і реалізації державних програм розробки систем національних інформаційних ресурсів.

Враховуючи викладене, розбудова правових засад інформаційної організації держави є поступальним кроком у сфері забезпечення інформаційної безпеки, запорукою стабільності в умовах зростання загроз міжнародного кібертероризму, кіберзлочинності, інформаційної експансії з боку РФ, ескалації діяльності екстремістських і сепаратистських рухів і організацій як усередині країни, так і за її межами.

Література

1. Про інформацію: Закон України від 2 жовтня 1992 року №2657 // Відомості Верховної Ради України. – 1992. - №48. – Ст.650

2. Інформаційна складова державної політики та управління: монографія / За загальною редакцією Грицяк Н.В.; Нац. акад. держ. упр. при Президентові України. — Київ: К.І.С., 2015. — 320 с.

3. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: рішення Ради Національної безпеки і оборони України від 28 квітня 2014 року, уведеного в дію Указом Президента України від 01.05.2014 № 449/2014

РИЗИКОВИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ОБСЯГУ ОПТИМАЛЬНИХ ІНВЕСТИЦІЙ У БЕЗПЕКУ ІНФОРМАЦІЇ

Архипов О., Архипова Є.
НТУУ «КПІ»

Одними з перших дослідників, які здійснили теоретико-методологічне обґрунтування граничного обсягу інвестицій у безпеку інформації, є американські вчені Л. Гордон і М. Лоеб. Згідно із їхнім дослідженням, оптимальний обсяг інвестицій в систему захисту інформації (СЗІ) не може перевищувати 36,79% від величини максимальних втрат, які можуть виникнути в разі реалізації загроз інформації. Проте Гордон і Лоеб не довели повноту та достатність запропонованої ними системи аксіом, що зумовило появу чисельних доповнень та модифікацій, а отже й різних висновків щодо величини граничних інвестицій у СЗІ, які, за деякими роботами, могли перевищувати 100 % від величини максимально можливих втрат. Причиною таких розбіжностей є формально-апроксимативний спосіб побудови функції ймовірності порушення захищеності інформаційних ресурсів, який не дозволяє врахувати відомості про реальні механізми розвитку та реалізації інформаційних загроз і ризиків.

Звернемося до моделі, запропоновані для дослідження економіко-мотиваційних відносин, характерних для ситуації «атака-захист» в інформаційній сфері [1; 2]. Вважатимемо, що D – загальна вартість витрат атакуючої сторони А на реалізацію загрози T відносно деякого інформаційного ресурсу I, який належить стороні В; g – отриманий при цьому «виграш» атакуючої сторони А, величина якого обумовлюється цінністю ресурсу I для зловмисника. Збитки, яких зазнала в цій ситуації сторона В (власник ресурсу I), тобто вартість ресурсу з точки зору його власника, оцінюється ним як q, а загальна вартість реалізованого комплексу захисних заходів дорівнює c.

В загальному випадку ймовірність реалізації загрози T відносно деякого інформаційного ресурсу I є добутком ймовірність активації (виникнення) загрози відносно інформаційного ресурсу (P_t) та ймовірність успішного використання зловмисником вразливостей інформаційної системи, яка містить ресурс I (P_v):

$$P_T = P_t P_v . \qquad (1)$$

Значення ймовірності P_v залежить від рівня захищеності інформаційної системи, який у свою чергу обумовлюється обсягом інвестувань c в СЗІ [1]:

$$P_v = \frac{q}{q + sc} , \qquad (2)$$

де s – коефіцієнт, яким визначає рівень ефективності інвестувань c в СЗІ, причому чим більше значення s, тим нижче величина ймовірності успішної

реалізації атак.

У разі відсутності цінної інформації в ІС ($q = 0$) ймовірність $P_v = 0$. Коли вартість q ресурсу I висока чи дуже висока, а витрати на СЗІ низькі ($q>>sc$), ймовірність $P_v \to 1$. Якщо власник ресурсу I адекватно враховує його цінність q та приділяє його захисту відповідну увагу, значення q і sc можуть виявитися співрозмірними, але при цьому завжди буде виконуватися вимога $0 < P_v < 1$. Припустимо, що при s=0 P_v =1, а вихідний інформаційний ризик $R_1 = P_t q$. Інвестування у СЗІ коштів у розмірі c (та їх раціональне використання) призводить до того, що ймовірність успішного використання вразливості стає меншою за 1, тобто P_v <1. Залишковий ризик в цьому випадку дорівнюватиме $R_T = P_t P_v q$, величина втрат, які вдалося попередити: $R_1 - R_T = P_t q - P_t P_v q = (1 - P_v) P_t q$, а відповідний «прибуток» $\Delta_R = R_1 - R_T - c = (1 - P_v) P_t q - c$. Замінюючи P_v його розгорнутим виразом (2), отримуємо:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R , \qquad (4)=3$$

Діапазон можливих значень c раціонально обмежити діапазоном «розумних» інвестицій: $0<c< q(s–1)/s$, при цьому коефіцієнт $s > 1$. Досліджуючи співвідношення (3) на екстремум (вважаючи, що Δ_R є функцією змінної c), отримуємо вираз: $\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0$, з умов виконання якого [1] визначаємо обсяг інвестицій c_{eff}, що забезпечує отримання найбільшого значення Δ_R:

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1), \qquad (6)=4$$

а також формули розрахунку значення ймовірності P_v і ризику R для оптимального обсягу інвестицій:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}, \; R_T(c_{eff}) = P_v(c_{eff}) P_t q = q\sqrt{\frac{P_t}{s}} . \qquad (7)=5$$

Аналіз формули (4) дає можливість оцінити максимальний обсяг інвестувань в СЗІ. Досліджуючи на екстремум залежність (4) як функцію змінної s, отримуємо:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2} s^{-3/2} \sqrt{P_t}) = 0 . \qquad (8)=6$$

З рівності (6) знаходимо, що свого екстремуму функція $c_{eff}(s)$ досягає при значенні $s = 4 / P_t$. Цьому значенню змінної s відповідає максимум

функції $c_{eff}(s)$:

$$\max[c_{eff}(s)] = c_{eff}(4/P_t) = 0,25qP_t. \qquad (9)=7$$

Очевидно, що найбільшою величина оптимальних інвестицій в СЗІ буде при P_t=1. Таким чином, максимальний обсяг оптимальних інвестицій в СЗІ дорівнює 0,25 вартості ресурсу з точки зору його власника. Отриману умову можна вважати формалізацією принципу розумної достатності при побудові СЗІ. Зазначимо, що з досвіду побудови СЗІ значення $s \geq 10 \div 45$ [1], а для високоефективних рішень $S = 40 \div 60$. Тому відповідно до формули (4) навіть при P_t=1 обсяг інвестицій в СЗІ може дорівнювати 11-13 % вартості ресурсу, що захищається.

Вираз (2) формує оцінку ймовірності успішного використання зловмисником вразливостей інформаційної системи головним чином на основі «внутрішніх» уявлень організації-власника ресурсу *I* (сторона В) про необхідний рівень захищеності цього ресурсу. Однак реальний ступінь захищеності ресурсу *I* значною мірою визначається інтенсивністю і силою атак сторони А, що залежать від її уявлень про цінність ресурсу *I*, тобто від величини *g*. Тому, якщо атакуюча сторона А точно ідентифікована і для неї достовірно відома величина *g*, можливо більш об'єктивною оцінкою ймовірності P_v є:

$$P_v = \frac{g}{g + sc}. \qquad (8)$$

За однакового розуміння цінності інформації сторонами А і В g=q. Але зазвичай ці сторони мають асиметричні уявлення про цінність інформації, що потребує вибору формули (2) чи (8). Для власника ресурсу *I* його цінність *q* зазвичай розраховується на основі аналізу вартісних аспектів створення цього ресурсу. Для атакуючої сторони А цінність *g* «добутої» інформації формується на основі ринкової вартості ресурсу *I* та кількості потенційних покупців, що бажають його придбати. Також «добута» стороною А інформація може бути інформацію з обмеженим доступом (ІзОД), витік якої може завдати шкоди ряду третіх сторін, які пред'являтимуть претензії стороні В, як такій, що не забезпечила збереження ІзОД. Обсяг претензій у грошовому еквіваленті у цьому випадку і становитиме *g* [2], причому оцінювання *g*, на відміну від *q*, характеризується багатоваріантністю, нестійкістю та поганою прогнозованістю.

Припустимо, що $g \neq q$, причому стороні В, що захищається, відома оцінка вартості ресурсу з точки зору зловмисника. Тоді, з урахуванням формули (8) отримуємо для співвідношення (3) нову форму подання:

$$-c + \frac{sc}{g + sc} P_t q = \Delta_R, \qquad (9)$$

а кінцеві вирази (4), (6) набудуть вигляду:

$$c_{eff} = \frac{q}{s}\sqrt{P_t s} - \frac{g}{s}, \qquad (10)$$

$$\max[c_{eff}(s)] = c_{eff}(4g^2 / P_t q^2) = 0,25 q^2 P_t / g\ . \qquad (11)$$

Найбільшою величина оптимальних інвестицій в СЗІ виявляється при $P_t = 1$ і складає $c_{eff\,\max} = 0,25 q^2 / g$. Розбіжність g і q може стати причиною недостатнього або надлишкового інвестування в СЗІ. Для отримання об'єктивних даних про ***найбільшу*** величину оптимальних інвестицій в СЗІ у разі $g > q$ бажано користуватися формулою (8) і отримуваними на її основі співвідношеннями, тому окрім відомостей про рівень втрат q сторони В, необхідна інформація про цінність ресурсу I для атакуючої сторони А. У разі $g \le q$ для оцінювання ***найбільшої*** величини оптимальних інвестицій в СЗІ слід використовувати співвідношення (7), враховуючи нестабільність отримуваних оціночних значень g. У зв'язку з цим цікавою є можливість застосування інших моделей, що описують альтернативні розглянутим імовірнісні параметри ризику.

Реалізація захисту інформації в організації можуть варіюватися у дуже широких межах, залежно від відношення організації до питань інформаційної безпеки (ІБ). Основним фактором, який визначає характер цих відносин, є ступінь (рівень) зрілості організації в аспекті ІБ [3]. Врахування цього фактору у формулі (2) здійснюється шляхом вибору значення коефіцієнта ефективності інвестицій s, зокрема, більш високому рівню зрілості організації відповідає більше значення s. Однак величина коефіцієнту ефективності інвестицій s залежить не тільки від поведінки сторони, що захищається В, але і від зусиль та цілеспрямованості дій атакуючої сторони А. Тому адекватний вибір значення s виявляється дуже складним завданням. Спростити його можна, використовуючи основні фактори, що визначають потенціал атакуючої сторони, безпосередньо для обчислення імовірнісних параметрів P_t та P_v оцінки ризику. Зокрема, для представленого вище опису ситуації «атака-захист» отримуємо:

$$P_t = \frac{g - D}{g} = 1 - \frac{D}{g}\ . \qquad (12)$$

Змістовний аспект отриманої формули пояснюється так: чистий прибуток зловмисника у разі успішної реалізації загрози становить різницю між очікуваним «виграшем» g від використання (реалізації) отриманого ресурсу I та витратами D зловмисника на реалізацію цієї атаки. Якщо цінність ресурсу I для атакуючої сторони досить велика, то можна припустити, що зловмисник намагатиметься використати будь-які шанси для реалізації цієї загрози. Навпаки, якщо цінність ресурсу I для нього незначна, то економічні мотиви для виникнення загрози практично відсутні.

Для ймовірності P_v врахування ресурсних можливостей атакуючої

сторони А здійснюється шляхом множення значення інвестицій *c* в знаменнику формули (2) на мультиплікатор *c* / *D*, що дозволяє врахувати інвестиції *D*, які здійснюються стороною А в реалізацію атаки:

$$P_v(c,D) = \frac{q}{q + s\frac{c^2}{D}}. \qquad (13)$$

Очевидно, що зростання витрат D обумовлює збільшення ймовірності P_v, тоді як збільшення інвестицій *c* у захист інформації дає протилежний ефект. Використання формул (12), (13) для обчислення ризику призводить до виразу виду:

$$R_T = P_t \frac{q}{q + s\frac{c^2}{D}} q = (1 - \frac{D}{g}) \frac{q^2 D}{qD + sc^2}. \qquad (14)$$

На жаль, застосування знайденого ризику (14) для подальшої реалізації оптимізаційної процедури не дозволяє отримати рішення у явному вигляді. Залежність $R_1 - R_T = (1 - P_v) P_t q$ після підстановки в неї виразу (14) набуває логістичного характеру, а аналіз нерівності $\Delta_R = R_1 - R_T - c \geq 0$ дає можливість лише визначити діапазон розумних інвестицій:

$$\frac{qP_t}{2}(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}) \leq c \leq \frac{qP_t}{2}(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}). \qquad (15)$$

Потреба обчислення квадратного кореня у формулі (15) обумовлює очевидне обмеження $1 \geq 4D / sqP_t^2$, яке трансформується у нерівність виду $D \leq 0,25 sqP_t^2$, що накладається на обсяг інвестицій атакуючої сторони А. Крім того, зловмисник очікує отримати від викраденої інформації більше, ніж він витратив на її викрадення. Дослідження співвідношення (14) при *D*=0 показує, що максимальне значення розумних інвестицій в СЗІ не повинно перевищувати обсягу потенційних втрат *q* у разі викрадення ресурсу *I*. Зі збільшенням значень *D*, при $D \to 0,25 sqP_t^2$ права і ліва межі діапазону (15) зближуються, при цьому в граничному випадку найбільша величина оптимальних інвестицій в СЗІ складе 0,5 вартості ресурсу з точки зору його власника.

Відзначимо, що наявність обмежень $D \leq 0,25 sgP_t^2$ і $g \geq D$ характерна для ситуації, коли атакуюча сторона А в своїх діях керується виключно принципом економічної доцільності (розумної достатності). Однак за певних обставин цей принцип може не виконуватися, зокрема у випадку виконання завдання найманим співробітником спецслужби, який у разі важливості поставленої перед ним задачі може розраховувати на широке залучення додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних,

оперативних. Якщо можливі витрати «зловмисника-виконавця» на отримання потрібного йому ресурсу практично нічим не обмежені, то ймовірність успішної реалізації атаки наближується до одиниці. В цій ситуації, якщо сторона, що захищається, створюючи свою СЗІ, виходить із принципу розумної достатності, ґрунтуючись виключно на власних («внутрішніх») уявленнях про цінність ресурсу *I*, успішна реалізація загрози атакуючої стороною А практично гарантована.

Література

1. Архипов О.Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О.Є. Архипов, А.В. Скиба // Захист інформації. – 2013. – Том15, №4. – С.366 – 375.

2. Архипов О.Є., Архипова Є.О. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів / О.Є. Архипов, Є.О. Архипова // Інвестиції: практика та досвід. – 2015. – №11. – С. 71-74.

3. Петренко С. А Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания АйТи, ДМК Пресс, 2004. – 384 с.

ПІДХІД ДО ВИЗНАЧЕННЯ ЕКСПЕРТНИХ ГРУП НА ОСНОВІ АНАЛІЗУ БАЗИ ДАНИХ «УКРАЇНІКА НАУКОВА»

Ланде Д.В., Балагура І.В.
Інститут проблем реєстрації інформації НАН України

Ефективний розв'язок задачі швидкого і кваліфікованого визначення експертних груп сприятиме ефективному вирішенню важливих завдань, які потребують залучення спеціалістів з різних галузей.Інформатизація людської діяльності зумовила значне збільшення кількості інформації, щодня виникають нові напрями наукових досліджень, що сьогодні унеможливлює пошук експертів за допомогою анкетування та опитування [1]. Актуальним завданням для дослідників є пошук компетентних експертів та формування експертних груп на основі інформаційних пошукових систем, соціальних мереж, наукових баз даних.

Закордонними вченими проведено ряд досліджень присвячених теоретичним аспектам та вимогам для виділення експертних груп. В тому числі у роботах [2, 3] описуються критерії погодження наукової і державної політики, а також промисловості для об'єктивного вибору експертів. В роботі [4] запропоновано підхід для пошуку експертів на форумах та у спеціалізованих соціальних мережах, де, на думку авторів, експерт може розкрити свої знання та спосіб мислення. Основні сучасні методи визначення експертів ґрунтуються на визначенні ключових слів та інформаційному пошуку у масивах інформації відповідних особистостей. В [5] автори пропонують пошук експертів на основі аналізу наукових текстів та побудови онтологій предметної галузі. В роботах [6, 7] підкреслюється важливість зв'язку науки, промисловості та виробництва задля прийняття важливих рішень та залучення експертів-науковців у всі галузі державної діяльності. Залучення науковців для прийняття важливих рішень необхідні в обороні держави, охороні здоров'я, промисловості. Значна кількість публікацій із даної тематики вітчизняних і зарубіжних науковців зумовлює актуальність представленої тематики.

Постановка завдання

Виявлення експертних груп може бути здійснено за допомогою визначення кластерів в мережі співавторства [8, 9]. Авторами запропоновано побудувати таку мережу на основі реферативної БД «Україніка наукова», яка є найбільшим політематичним ресурсом в Україні. Сьогодні реферативна база даних «Україніка наукова» нараховує понад 571 598 записів. Даний реферативний ресурс створено у 1998 році для забезпечення вільного доступу до інформації про результати наукової діяльності вітчизняних учених і фахівців, на основі розвинення українського

реферативного журналу «Джерело». Цьогоріч український реферативний журнал «Джерело» святкує своє 20-річчя [10].

В роботі [9] запропоновано методику наукометричного аналізу на основі поєднання мереж співавторів та мереж термінів. Представлений алгоритм є основою для визначення експертних груп у даній роботі. Детальний наукометричний аналіз окремого наукового напряму чи галузі дає змогу визначити найбільш впливових науковців та тематику їх досліджень. Саме поєднання методів аналізу мереж співавторів та термінів для аналізу баз даних наукових публікацій надає змогу визначити найбільш компетентних експертів в окремих наукових напрямах за визначеною тематикою. Методам аналізу мереж співавторів присвячено багато зарубіжних наукових праць [11, 12]. В Україні дослідження мереж співавторів також проводять й іншими, в тому числі: Майстренко О.С. в дисертації провів дослідження мереж співавторів для вибраних науковців із НТУУ «КПІ», Мриглод О.І. побудувала мережі співавторів для вибраних наукових видань [13, 14].

Методика визначення експертних груп в своїй основі містить 4 етапи, що включають методи складних мереж, методи фільтрації тексту, візуалізацію даних.

В попередніх роботах [9] наведено методику досліджень та представлено відповідні дослідження реферативної бази даних «Україніка наукова» перших двох етапів.

На першому етапі визначається галузь та наукові напрями, за якими буде проведено аналіз, завантажується та фільтрується файл із реферативною інформацією. Результатом першого етапу є матриця мережі – відфільтровані за певними науковими напрямками дані про авторів та зв’язки між ними [8].

Другим етапом є створення мережі співавторів досліджуваної галузі, визначення основних характеристик мережі. У ході другого етапу визначаються основні властивості співробітництва науковців, наукові групи та найбільш комунікативні науковці за певним науковим напрямком [15].

На третьому етапі відбувається відбір рефератів наукових публікацій найбільш комунікативних науковців та створення текстового корпусу для виділення основних термінів за науковими напрямками [16].

На четвертому етапі проводиться візуалізація мереж термінів науковців та галузі в цілому, розрахунок основних параметрів та виділення опорних слів і відповідних словосполучень, автоматизоване формування термінологічної основи онтології наукових напрямків та експорт даних до редакторів онтологій. Проводиться узагальнення результатів, опис основних характеристик, тенденцій в галузі, остаточне погодження експертного колективу [9].

Результатом роботи має бути перелік науковців, що можуть бути експертами в заданому напрямі та перелік основних термінів, які відповідають тематиці робіт експертів.

Результати досліджень

Відповідно до третього етапу запропонованої методики, необхідно провести відбір рефератів наукових публікацій найбільш комунікативних науковців. У дослідженні використовувались реферати наукових колективів чотирьох провідних авторів з інформатики українською мовою, представлені в реферативній БД «Україніка наукова». Колективи авторів визначались на основі аналізу мереж співавторів та виділення найбільш важливих вузлів за характеристиками центральності [15]. Для кожної групи науковців було сформовано текстовий корпус, що містив близько 35 рефератів статей у фахових журналах, тез доповідей на конференціях та монографій. При попередній обробці тексту було вилучено нетекстові символи та виконано стеммінг.

Основні терміни та термінологічні словосполучення визначались за допомогою статистичного метода TF-IDF та методу «сигма». При подальшому обробленні для послідовності термінів та їх вагових значень будуються компактифіковані графи горизонтальної видимості та виконується перевизначення значень вагових коефіцієнтів. Далі експертним методом та за допомогою стоп-словника обираються основні терміни, що використовує автор [16].

Наступним етапом є представлення мережі термінів наукових колективів та їх аналіз. Відібрані терміни використовуються для створення мережі термінів, де вузлами є терміни та словосполучення, а зв'язки відповідають входженню термінів до словосполучень.

Основні терміни складаються із одного, двох та трьох слів та описуються за допомогою матриці інцидентності A, а матриці A^TA та AA^T містять асоціативні зв'язки першого (якщо два терміни утворюють третій) та другого (якщо термін утворений двома іншими) роду [15]. На рис. 1 наведено мережу термінів із асоціативними зв'язками.

Найбільш значимі слова і словосполучення в мережі термінів можна виділяти за допомогою алгоритма HITS (hyperlink induced topic search). Алгоритм HITS заснований на визначенні «авторитетних вузлів» (вузлів, на які багато посилань) та «вузлів-посередників» (вузли, що найбільш часто посилаються на інші). Для наукового колективу автора Петрова В.В. найбільш значимі терміни наведені у таблиці 1. Таким чином даний науковий колектив необхідно залучати при вирішенні завдань запису, зберігання, зчитування інформації, використання оптичних носіїв.

За допомогою перетину мереж термінів окремих колективів авторів можна визначити основні терміни наукового напряму, в якому вони працюють. Така мережа дає можливість визначити загальні напрями експертних груп або сформувати колектив із окремих експертів, що охоплюють декілька напрямів досліджень.

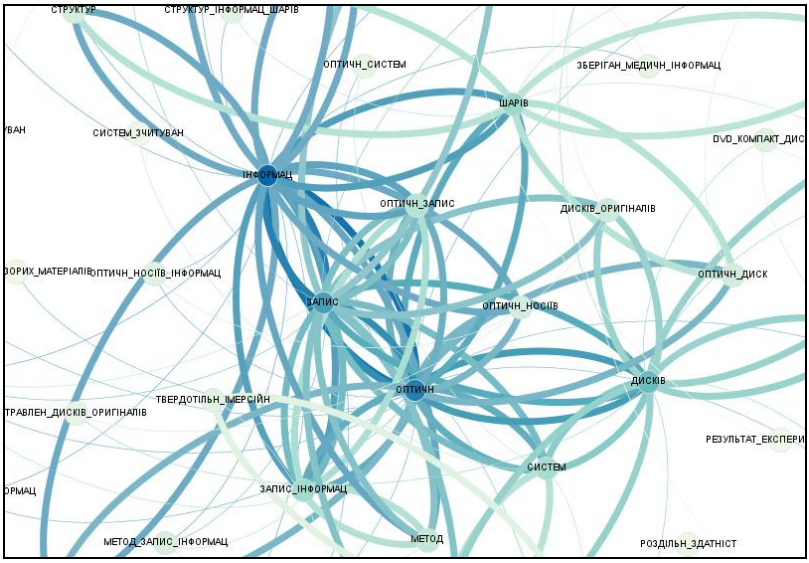


Рис. 2. Мережа термінів на основі аналізу публікацій наукового колективу Петрова В.В.

Таблиця 1

Терміни з найбільшим значенням авторства та посередництва

Терміни з найбільшим значенням авторитетності	Терміни з найбільшим значенням посередництва
оптичн_запис_інформац	інформац
оптичн_зчитуван_інформац	оптичн
оптичн_носіїв_інформац	запис
інформац_оптичн_носіях	запис_інформац
метод_запис_інформац	дисків
запис_інформац	оптичн_запис
оптичн_запис	систем
структур_інформац_шарів	зберіган_інформац
термін_зберіган_інформац	шарів
довготермінов_зберіган_інформац	зчитуван_інформац
зберіган_медичн_інформац	оптичн_носіїв
зчитуван_інформац	метод
зберіган_інформац	структур

Отримані терміни за окремими науковими напрямами та дані про їх зв'язки входження та асоціативні зв'язки можуть виступити термінологічною основою онтології, де терміни можуть виступати як класи онтологій, а асоціативні зв'язки – як відношення між ними. Така термінологічна основа онтології потребує подальшого експертного аналізу та розширення і дозволяє формалізувати науковий напрямок окремих наукових груп.

В результаті роботи визначено чотири наукові колективи, які можуть виступати в якості експертних груп для вирішення завдань пов'язаних із комп'ютерними науками. Визначені терміни надають можливість коректно визначати галузь діяльності відповідних експертів.

Висновки

В роботі показано можливість пошуку експертних груп на основі мереж співавторів з використанням мереж термінів. Запропоновано технологію наукометричного аналізу для вдосконалення інструментарію вітчизняної реферативної бази, покращенню якості інформаційного сервісу та ефективності аналітичної діяльності. Результати досліджень дають можливість обґрунтувати, автоматизувати та прискорити процедуру підбору компетентних експертів, що входитимуть до складу сформованих галузевих груп. Зокрема, результати роботи дозволять проводити пошук експертів-науковців для державних завдань, що потребують швидкого реагування на події, пошук наукових колективів та шкіл для вирішення технічних завдань, зокрема в оборонній галузі.

Література

1. Рогушина Ю.В. Використання організаційних онтологій для пошуку експертів у нових предметних областях / Ю.В. Рогушина, А.Я. Гладун // Проблеми програмування. – 2007. – №1. – С.73–83.

2. Jianshan S. Leverage RAF to find domain experts on research social network services: A big data analytics methodology with MapReduce framework / Sun Jianshan, Xu Wei, Ma Jian, Sun Jiasen // Int. J. Production Economics. – 2015. – № 165. – P.185–193.

3. Rowe S. How experts are chosen to inform public policy: Can the process be improved? / Silvia Rowe, Nick Alexander, others // Health Policy. – 2013. – № 112. – P.172–178.

4. Wei Ch.-P. Finding experts in online forums for enhancing knowledge sharing and accessibility / Chic-Ping Wei, Wen-Ben Lin, others // Computers in Human Behavior – 2013. – № 112. – P.325–335.

5. Крюков К.В. О понятии формальной компетенции научных сотрудников / К.В. Крюков, О.П. Кузнецов, В.С. Суховеров // Материалы III международной научно-технической конференции (г. Минск, 21-23 февраля 2013 г.) – М.: БГУИР, 2013. – С.143–146.

6. Liu D.-R. Integtating expert profile, reputation and link analysis for expert finding in question-answering websites / Duen-Ren Liu, Yu-Hsuan Chen, Wei-Chen Kao, Hsiu-Wen Wang // Information Processing and Management. – 2013. – № 49. – P.312–329.

7. Zhou G. An empirical study of topic-sensitive probabilistic model for expert finding in question answer communities / Guangyou Zhou, Jun Zhao, others // Knowledge-Based Systems. – 2014. – № 66. – P.136–145.

8. Горбов І.В. Визначення потенційних експертних груп науковців в мережі співавторства з використанням методів підтримки прийняття рішень / І.В. Горбов, С.В. Каденко, І.В. Балагура, Д.Ю. Манько, О.В. Андрійчук // Реєстрація, зберігання і обробка даних. – 2013. – Т.15, №4. – С.87–97.

9. Балагура І. В. Лінгвістичні дослідження взаємозв'язків науковців на основі аналізу реферативної бази даних «Україніка наукова» / Балагура І. В., Ланде Д. В.// Реєстрація, зберігання і обробка даних. – 2014, – Т.16, №3 – С.45–53.

10. Корпоративний проект «Система реферування української наукової літератури» [електронний ресурс]:[сайт] – Режим доступу: http://www.nbuv.gov.ua/node/522.

11. Alireza A. Betweenness centrality as a driver of preferential attachment in the evolution of research collaboration networks / Abbasi Alireza, Hossain Liaquat, Loet Leydesdorff // Journal of Informetrics. – 2012. – V. 6, № 3. – P. 403–412.

12. Leydesdorff L. Eugene Garfield and algorithmic historiography: Co-Words, Co-Authors, and Journal Names / Loet Leydesdorff // Annals of Library and Information Studies. – 2010. – V.57, №3. – P.248–260.

13. Майстренко О.С. Бізнес-моделювання слабко структурованих організаційних систем : автореф. дис. … канд. техн. наук : 01.05.04 / О.С. Майстренко ; НТУУ «КПІ». – К., 2013. – 24 с.

14. Мриглод О.І. Елементи кількісного аналізу наукових періодичних видань / О.І. Мриглод // Наука України у світовому інформаційному просторі. – 2014. – Вип. 10. – С.19–28.

15. Балагура І.В. Дослідження параметрів важливості вузлів в мережах співавторів /І.В. Балагура, Д.В. Ланде, І.В. Горбов // Реєстрація, зберігання і обробка даних. – 2013. – Т.15, №1 – С.45-52.

16. Ландэ Д. В. Подход к созданию терминологических онтологий /Д. В. Ландэ, А. А. Снарский // Онтология проектирования – 2014. – Т.12, №2 – С.83–92.

ЖИВУЧІСТЬ ІНФОРМАЦІЙНИХ ПОТОКІВ У СУЧАСНИХ СЕРЕДОВИЩАХ

Березін Б.[1], Ланде Д.[1],
Павленко О.[2]
[1]ІПРІ НАН України,
[2]Відкритий міжнародний університет розвитку людини "Україна"

Постановка проблеми, її актуальність та аналіз публікацій Сучасний інформаційний простір є динамічною системою, яка складається з інформаційних елементів (документів) пов'язаних між собою за тематикою. Більшість інформаційних ресурсів, які на сьогодні публікують та зберігають інформацію в цифровому вигляді, розміщують інформацію он-лайн чи на цифрових носіях та мають потокову структуру [1]. Прикладами таких ресурсів є соціальні мережі, стрічки новин, блоги. Публікацію наукових статей також можна розглядати як інформаційний потік (ІП) – тобто послідовність документів, які відповідають певній тематиці та можуть розміщуватися на веб-серверах інституційних репозитарієв. Нарешті, документи, що розміщуються для довготермінового або постійного зберігання в електронних, комп'ютерних бібліотеках, архівах, страхових фондах тощо, теж мають зазвичай форму ІП. Такому тематичному ІП ставлять у відповідність часовий ряд, який складається з кількості повідомлень або документів опублікованих за певний проміжок часу. Поняття живучості інформаційних об'єктів в Інтернет-середовищі чи на носіях має на увазі їх здатність своєчасно виконувати свої функції (інформування) в умовах дії дестабілізуючих факторів. Такими факторами можуть бути їх усунення з інформаційного простору, втрата ними властивостей актуальності, доступності [2,3].

В роботі розглядається живучість ІП у різних видах сучасних середовищ: живучість ІП новин з веб-сторінок соціальної мережі Twitter; живучість ІП наукових публікацій (НП) з сторінок відповідних веб-репозитарієв, електронних бібліотек в Інтернеті; живучість ІП ресурсів на оптичних носіях, що довготерміново зберігаються в комп'ютерних та електронних архівах, страхових фондах. Існування ІП у різних середовищах передбачає подолання різних видів загроз: пошкодження носіїв інформації/обладнання, старіння носіїв/обладнання, старіння програмного забезпечення/форматів, помилки операторів, атаки, природні катастрофи, економічні помилки і т.і., тобто передбачає забезпечення живучості цих ІП. На сьогодні більшість досліджень в області інформаційних потоків присвячена новинним ІП. (В роботі [4] запропанована логістична модель для розгляду динаміки новинних ІП, в роботах [2-3] розглядається живучість повідомлень, роботи [1,5] стосуються аналізу новинних ІП). В той же час, живучість ІП НП, ІП на носіях детально не досліджені.

Метою роботи є розробка методологічних засад забезпечення живучості інформаційних потоків у різних сучасних середовищах на основі аналізу характеристик ІП та розробки відповідних моделей для оцінки живучості ІП.

Характеристики ІП та моделі для оцінки їх живучості

Аналіз показує, що серед основних особливостей вищезазначених ІП, які впливають на їх живучість, можна виділити доступність, републікацію, індексованість та поширеність форматів даних.

Доступність. Оцінка живучості ІП в Інтернет-середовищі залежить від доступності веб-серверів, на яких розміщені інформаційні елементи (ІЕ). Для визначення характеру цієї залежності було налагоджено моніторинг стану сайтів, на яких може бути розміщено контент. На основі акопиченого матеріалу було розраховано дані й побудовано розподіли випадкових значень показника доступності й недоступності сайтів, а також періодів їх доступності та недоступності [6] (відповідні ранжирувані розподіли можуть бути апроксимовані експоненціальною та степеневою функціями).

Оцінка живучості ІП на оптичних носіях залежить від їх доступності, тобто можливості зчитування файлів. Внаслідок особливостей технології запису інформації, оптичні диски вміщують деяку кількість помилок, число яких зростає в процесі довготермінового зберігання. Можливості системи корекції стандартного оптичного приводу обмежені, тому наявність помилок характеризує зниження функціональності носіїв інформації. Для визначення живучості інформації на оптичних дисках з точки зору доступності може використовуватися показник помилок. (Для DVD це PI Sum8, його максимально допустиме значення складає 280). Для колекції CD та DVD дисків було проведено тестування помилок. Аналіз розподілів вибірок оптичних дисків, ранжируваних за кількістю помилок, показав можливість їх апроксимації степеневою функцією [7]. Доступність ІЕ на сапфірових дисках для архівного зберігання [8,9] може оцінюватися за допомогою показника помилок PI Sum8 (який характеризує відповідність записаної інформації основним вимогам стандарту DVD) з врахуванням часової стабільності металевого відбиваючого покриття.

Републікація. При користуванні інформаційними ресурсами в мережі Інтернет може відбуватися копіювання, розмноження їх версій, тобто републікація. Оцінка живучості ІП в Інтернет-середовищі в значній мірі залежить від кількості версій ІЕ. В ІП новин з соціальної мережі Twitter в якості показника републікації для твітів може бути використано значення ретвітів. Для визначення характеристик процесу републікації контенту ІП НП в Інтернет використовувалися запити до пошукової системи Google Scholar для отримання списку публікацій з заданої тематики на протязі періоду в один рік [6]. В отриманому списку публікацій аналізувалось поле “всі версії статті” та були проранжирувані кількості версій НП по вибраній тематиці в Інтернет за рік. Отримані таким чином розподіли для вибірок розміром біля 100 НП в усі роки інтервалу 1998 – 2013 р.р. були

апроксимовані за допомогою експоненціальної функції. Для ІП на оптичних носіях в якості характеристики републікації може використовуватися кількість копій носіїв (які доцільно зберігати в різних сховищах).

Індексованість. Оцінка живучості ІП при довготерміновому зберіганні в Інтернет-середовищі також залежить від індексованості веб-серверів, на яких розміщені ІЕ потоків. Індексованість новинних ІП мережі Twitter забезпечується пошуковими системами Google, Yandex, Meta тощо. Для визначення характеру цієї залежності для ІП НП було використано запити до пошукових систем Google та Scholar Google. Результати показують, що доля файлів, проіндексованх в Scholar Google по відношенню до файлів, проіндексованх Google, може змінюватися від одиниц до десятків відсотків, в залежності від конкретного електронного архіву. Відповідно, може змінюватися властивість НП виконувати свої функції, тобто живучість. Для більшої живучості ІП на носіях, інформація про них повинна бути доступна в Інтернет або у спеціальних системах. Наприклад, для Страхового фонду документації (СФД) [9] ведеться державний реєстр документів СФД – автоматизована система з обмеженим доступом (на початок 2013 р. до неї було внесено більше 33 тис. документів).

Поширеність та стабільність форматів. Оцінка живучості ІП в Інтернет-середовищі або на носіях також може залежати від поширеності форматів, використаних для їх представлення. Тобто, на їх живучість може впливати старіння форматів, в яких представлені ці ІП (поява нових форматів, ПЗ і обладнання, несумісного зі старими форматами представлення даних). В роботі [6] наведено результати аналізу щодо поширеності форматів в Інтернет (html – 90%, pdf – 2%-3% тощо), а також поширеності версій формату pdf (1.0, 1.1, 1.2, 1.7 - одиниці відсотків, 1.3-1.6 десятки відсотків ресурсів).

Для забезпечення доступу до інформації через значний інтервал часу необхідно використання стабільних форматів представлення даних, що дозволяє істотно подовжити час між послідовними конверсіями електронних документів та зробити цей процес більш передбачуваним. Використання відкритих форматів (наявність вичерпного опису, відсутність правових обмежень і т.і.) гарантує, що за певних зусиль документи можна буде прочитати навіть через тривалий час. До міжнародних стандартів відкритих форматів документів відносять формати серії pdf.

Моделі для оцінки живучості ІП. Із-за протяжності у часі ІП його елементи мають мережеву структуру, тобто більш нові елементи потоку можуть посилатися на ресурси попередніх елементів. (У текстах новинних повідомлень – посилання на попередні новини, на веб-сторінки, відео тощо, у текстах наукових публікацій – посилання на публікації, презентації, додатки і т.і., в текстах геологічних звітів на оптичних носіях - посилання на публікації, на попередні звіти тощо.)

На основі наведених вище особливостей представлення ІП в середовищі Інтернет та на носіях, будемо вважати, що живучість ІЕ залежить від слідуючих основних факторів:

- живучості тексту ІЕ, на яку впливають кількість копій публікації в Інтернет-середовищі та на носіях (в загальному випадку будемо розглядати кількість версій публікацій, тобто не лише повнотекстові копії, а й анотації статей); доступності серверів, на яких зберігаються копії та версії ІЕ; індексованості тексту публікації в універсальних, наукових та спеціальних пошукових системах; поширеності формату, в якому представлено текст тощо;
- частки доступних посилань, що використовуються в ІЕ;
- живучості ІЕ, на які є посилання в тексті розгядаємого ІЕ (теж залежить від кількості копій, версій, доступності серверів, індексованості, поширеності форматів тощо).

З урахуванням вище наведеного, живучість ІЕ при довготерміновому зберіганні в Інтернет-середовищі або на носіях можна оцінювати на основі кількості версій ІЕ та її посилань в Інтернет/на носіях. Живучість ІЕ будемо представляти двома значеннями: живучістю тексту ІЕ та живучістю її посилань.

Живучість тексту ІЕ будемо оцінювати кількістю версій ІЕ з урахуванням доступності, індексації та поширеності формату:

$$ST = \sum_{i=1}^{VT} AT_i * IT_i * PFT_i \qquad (1)$$

ST – живучість тексту ІЕ;

AT_i – доступність i-ї версії тексту ІЕ;

IT_i – індексованість в пошуковій системі i- ї версії тексту ІЕ;

PFT_i – поширеність формату i-ї версії тексту ІЕ в Інтернет.

Живучість посилань ІЕ будемо оцінювати усередненою кількістю версій посилань з урахуванням доступності та індексації, а також з урахуванням загальної частки доступних посилань.

$$SR = \frac{RRL}{RRC} * \frac{\sum_{j=1}^{RRL} \sum_{i=1}^{VR_j} AR_{ij} * IR_{ij} * PFR_{ij}}{RRL}, \qquad (2)$$

SR – живучість ресурсів, на які посилається ІЕ;

AR_{ij} – доступність i–ї версії j–го ресурсу, на який посилається ІЕ;

IR_{ij} – індексованість в пошуковій системі *i* -ї-версії *j* – го ресурсу, на який посилається ІЕ;

PFR_{ij} – поширеність формату *i* - ї версії *j* – го ресурсу ІЕ в Інтернет.

VR_{ij} – кількість версій *j* –го ресурсу, на який посилається ІЕ;

RRL – кількість "живих" посилань, на який посилається ІЕ;

RRC – загальна кількість Інтернет-посилань, які є в ІЕ.

Методологічні засади забезпечення живучості інформаційних потоків

В роботах [2,3,6] розглянуто кілька механізмів, що забезпечують живучість інформаційних потоків в Інтернеті. Зазвичай, ці механізми використовуються не в чистому вигляді, а комбінуються. Дзеркальне копіювання даних при розміщенні їх на цільовий ресурс. Тобто автор розміщує інформацію, яка копіюється хостинг-провайдером на деяку кількість дзеркальних серверів. (Приклад – відома служба WikiLeak, використовує кілька сотень серверів-дзеркал). Передрук інформації (републікації, «копіпаст») на інші сайти з метою їх інформаційного наповнення. Найбільш важлива і цікава інформація передруковується сотні разів, у той час як неактуальна, нецікава інформація практично не дублюється. Розміщена одного разу інформація назавжди потрапляє в архівні служби Інтернету типу Internet Archive. Інформація індексується глобальними пошуковими системами типу Google, Яндекс та залишається у їх кеш-пам'яті, звідки вона доступна користувачам.

І нарешті, інформація з веб-сайту може зберігатися на локальних комп'ютерах кінцевих користувачів, які отримали до неї доступ або безпосередньо, або через інтеграторів інформації.

Особливості оцінки живучості НП з використанням запропанованої вище моделі може бути показана на прикладі наукової періодики України, представленої на сайті Національної бібліотеки України імені В.І. Вернадського. Для вибірки НП окремого наукового видання з цього електронного архіву середнє значення кількості версій НП в Інтернет середовищі складає приблизно 2 (на основі даних пошукових систем Google Scholar та Google, аналізувалися 2008-2010 р.р.). Доступність серверів, на яких зберігаються версії НП видання наукової періодики України може оцінюватися за допомогою сервісу http://uptimerobot.com. Індексованість НП в електронному архіві наукових публікацій є незначною. Для порівняння оцінювалась також середня кількість версій НП в Інтернет-середовищі для одного з найбільших електронних архівів наукових публікацій (http://arxiv.org). Для вибірки за 2008-2010 р.р. вона складає біля 7. Враховуючи те, що кількість версій НП є однією з основних складових живучості, це показує порівняно невисокий рівень живучості НП

періодичних видань України при довготерміновому зберіганні в Інтернет-середовищі. Виходячи із запропанованої структури живучості НП, серед основних шляхів її підвищення: збільшення кількості версій НП в Інтернет-середовищі; підвищення доступності серверів, де розміщуються версії НП; підвищення рівня індексованості НП в пошукових системах; використання більш нових форматів тощо.

Доцільним напрямком збільшення кількості версій НП є використання архівних сервісів мережі Інтернет (webarchive.org, webcite.org та деяких інших) поряд з розміщенням додаткових версій НП у відкритих репозитаріях, що створюються в університетах та інших наукових установах. Але, при використанні архівних сервісів для збільшення кількості версій НП важливо забезпечити їх індексацію, тобто представлення їх адрес у результатах обробки запитів пошуковими системами. Рішенням цієї проблеми може бути розміщення адрес копій в полях метаданих НП (наприклад, в міжнародному стандарті метаданих для архівних матеріалів ISAD (G) передбачені дані про наявність та місцезнаходження копій).

Інструментальні засоби моніторингу інформаційних потоків

Для отримання статистичних даних про ІП з метою побудови моделей живучості, створюються відповідні програмні засоби. Програма моніторингу для соціальної мережі Twitter розроблена на R-мові програмування та забезпечує збір даних про ретвіти та вибране з новинних повідомлень мережі. Для збору даних про ІП наукових публікацій на R-мові створюється програмні засоби доступу до сервісу Google Scholar Citations. При цьому було використано також набір дистрибутивів Денвер для налагодження веб-додатків на локальному ПК. Для тестування показників помилок при зберіганні інформації на оптичних дисках було використано програму Opti Drive Control 1.51, пакет PlexTools Professional V2.12, та деякі інші засоби.

Висновки

В роботі визначено особливості представлення ІП в мережі Інтернет та на оптичних носіях, які впливають на живучість ІП: републікація; доступність серверів, на яких зберігаються ІП; індексація ІП в пошукових системах; поширеність форматів даних. На базі цих особливостей запропановано моделі для оцінки живучості ІП в Інтернет-середовищі та на носіях, показано їх можливості на прикладі української наукової переодіки.

Використання цих моделей для оцінки живучості ІП дозволяє сформулювати рекомендації по підвищенню їх живучості на основі збільшення кількості версій ІЕ, підвищення доступності та індексованості цих версій, впровадження сучасних форматів даних або конвертації форматів.

Література

1. Kleinberg J. Temporal dynamics of on-line information streams // Data Stream Management: Process-ing High-Speed Data Streams. — Springer, 2006. —18 p.

2. Додонов А.Г., Ландэ Д.В. Живучесть информационных объектов в сети Интернет // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2013): материалы III междунар. науч.-техн. конф. (Минск 21-23 февраля 2013 года) / - Минск: БГУИР, 2013. - С. 457-460.

3. Додонов А.Г., Ландэ Д.В. Живучесть информационных сообщений в Интернет-среде //Комп'ютерні системи та мережні технології (CSNT-2012): тези доповідей V міжнародної науково-технічної конференції. м. Київ, 13-15 червня 2012 р. Національний авіаційний університет. - К.: НАУ, 2012. - С. 49-51.

4. Ландэ Д.В. Основы интеграции информационных потоков: Монография -К.: Инжиниринг, 2006. - 240 с.

5. Baranovskiy O. Recurrence plots as method for information flows analysis// The Advanced Science Journal, Volume 2015, Issue 2. – P.45-49

6. Ланде Д.В., Березін Б.О. Підхід до оцінки живучості наукових публікацій при довготерміновому зберіганні в інтернет-середовищі // Реєстрація, зберігання і обробка даних, 2014. - Т. 16. - N 4. - С. 34-43.

7. Березін Б.О., Ланде Д.В. Дослідження стану оптичних носіїв при довгостроковому зберіганні цифрової інформації // Студії з архівної справи та документознавства / Держ. архів. служба України, УНДІАСД. - К., 2012. - Т. 20. - С. 133-139.

8. Петров В.В., Семиноженко В.П. Новітня технологія довготривалого зберігання інформації на сапфірових оптичних дисках//Вісн. НАН України, 2014, № 4 – С. 24-32.

9. Березін Б.О., Ланде Д.В., Шиховець О.В. Живучість інформаційних об’єктів при довготерміновому зберіганні із використанням архівних носіїв //Информационные технологии и безопасность: основы обеспечения информационной безопасности: Материалы международной научной конференции ИТБ-2014. - К.: ИПРИ НАН Украины, 2014. - С. 40-45.

10. Гриценко М.О., Полонський О.І., Піскачов О.І. Створення страхового фонду документації – одна із складових національної безпеки держави // Страховий фонд документації, 2014. - N 2. - С. 25-31.

О МОДЕЛИРОВАНИИ СИСТЕМЫ УПРАВЛЕНИЯ КАЧЕСТВОМ ИНФОРМАЦИОННЫХ УСЛУГ

Ю.Б. Бояринова, Н.А. Городько
Інститут проблем реєстрації інформації НАН України

1. Постановка проблемы

В связи с неуклонным развитием информационных технологий в различных областях деятельности все актуальнее становится вопрос о качестве информации необходимой для решения конкретной задачи или достижения некой цели.

Общеизвестно, что структура и объемы информационных потоков, которые необходимо обрабатывать, требуют наличия эффективных методов и алгоритмов их обработки, хранения и контроля. Что и предопределяет необходимость создания эффективной системы, которая контролирует и обеспечивает качество информационных услуг.

Информационная услуга – услуга ориентированная на удовлетворение информационных потребностей пользователей путем предоставления информационных продуктов; действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами [1]

Современные системы управления базируются на принципах общеорганизационного метода повышения качества (TQM — Всеобщего управления качеством). [2]

Несмотря на то, что существует множество систем управления качеством, к сожалению, во многих случаях разработчики сталкиваются с проблемой выбора системы, которая отвечает всем предъявляемым требованиям и способна удовлетворить установленные или прогнозируемые потребности пользователей. Поэтому, по-прежнему актуальным остается решение проблем, которые связаны с моделированием систем управления информационными сервисами.

2. Цель работы

Необходимым условием эффективного функционирования информационных сервисов (ИС) является наличие систематизированного набора средств, которые собирают сведений об объемах обрабатываемой информации, распределяют потоки информации во времени и пространстве и т.д. Управление процессами ИС предполагает также наличие средств воздействия на поведение объектов с целью принятия управленческих решений, направленных на достижение оптимального взаимодействия всех взаимосвязанных элементов.

Основная цель моделирования систем управления информационными сервисами (СУ ИС) определяется, как поиск оптимального или наилучшего

(субоптимального) результата выполнения управления процессами. Для этого необходимо определить набор составляющих операций процесса, порядок и правила их выполнения, механизмы контроля и управления в рамках процесса, параметры, характеризующие выполнение операций и процесса в целом, а так же результатов выполнения процессов.

3. Процессный подход к моделированию систем управления качеством информационных услуг

С точки зрения теории управления каждый процесс СУ ИС можно рассматривать, как объект управления (ОУ), который представляет собой структурированную совокупность действий, спроектированную для достижения конкретной цели. При этом каждый процесс преобразует один или несколько определенных входов в определенные выходы. Они могут включать в себя любые роли, ответственности, инструменты и контроли управления, необходимые для надежного получения выходов. При необходимости, процесс может определять политики, стандарты, рекомендации, виды деятельности и рабочие инструкции [3].

В зависимости от сложности процесса последовательность действий, составляющих процесс, может быть объединена в подпроцессы или суб-процессы. Последовательность действий моделируется на разных уровнях абстракции. На самом верхнем уровне отображаются только наиболее важные шаги процесса. Глубина декомпозиции каждого из высокоуровневых шагов (подпроцессов) определяется сложностью процесса и требуемой степенью детализации. Для того чтобы получить действительно полное представление о процессе, производится декомпозиция до атомарных функций — хорошо понятных элементарных действий (отдельных операций), которые нет смысла раскладывать на составляющие.

Как и в любой системе, внутренние связи между действиями в процессах СУ ИС сильнее внешних. Следовательно, процесс можно рассматривать как замкнутое объективное единство связанных друг с другом ОУ, упорядоченных по определенному закону или принципу. Общеизвестно, что основой упорядочения является цель функционирования.

Каждый ОУ процесса СУ ИС размещается и функционирует в некоторой вполне определенной внешней среде. Их взаимодействие с внешней средой осуществляется через вход и выход. Под входом при этом понимается точка или область воздействия извне; под выходом – точка или область воздействия вовне.

Таким образом, каждый процесс (действие) СУ ИС характеризуется следующими группами переменных:

- входные, которые генерируются ОУ, внешними относительно исследуемого;
- выходные, т.е. интегрируемые исследуемым ОУ;
- состояния, которые характеризуют динамическое поведение исследуемого ОУ.

Все три группы величин предполагаются функциями времени. Воздействуя на входы ОУ, мы переводим его из одного состояния в другое и тем самым получаем изменения на выходах, что фиксирует его новое состояние.

Перевод ОУ из одного состояния в другое сопровождается затратами ресурсов, которыми он обладает. Управление принято называть оптимальным, если перевод ОУ из одного состояния в другое, которое соответствует достижению цели и будет сопровождаться минимальными затратами.

Рассмотрим некоторый объект, подверженный действию внешних измеряемых и неизменяемых возмущений и управляющих воздействий. Предположив, что все измерения и формирование управляющих воздействий осуществляется синхронно с некоторым периодом T_0 (обычно $T_0 \equiv const$) в дискретные моменты времени $\bar{t} = tT_0$ ($t = 0,1,2,...$), представим его математическую модель в форме эволюционного уравнения

$$y_t = Y(y_0^{t+1}, u_0^{t-d-1}, w_0^t, v_0^t, d, \Theta) \ , \qquad (1)$$

определяющего последовательность выходных переменных $\left\{ y_t \right\} \overset{def}{=} y_0, y_1, ...$ при заданных начальных условиях, последовательности управляющих воздействий $\left\{ u_t \right\} \overset{def}{=} u_0, u_1, ...$ и имеющихся последовательностях $\left\{ w_t \right\} \overset{def}{=} w_0, w_1, ...$, $\left\{ v_t \right\} \overset{def}{=} v_0, v_1, ...$ измеряемых и неизмеряемых возмущений соответственно (переменные y_t, u_t, w_t, v_t – скалярные или векторные величины). В этом уравнении Θ – вектор параметров объекта; Y – некоторый оператор над стоящими в скобках аргументами.

$d = ent(\tau / T_0)$ – целое неотрицательное число, которое определяет величину запаздывания по управляющему входу, выраженную в числе интервалов дискретности, где $\tau > 0$ - величина чистого запаздывания.

Пусть U обозначает множество всех возможных значений управления u_t в каждый момент времени t, так что $u_t \in U$ для всех t. В общем случае применительно к многомерному (векторному) объекту с N каналами передачи управляющих воздействий имеем $U \subseteq R^N$.

Допустимыми будем считать любые управления $u_t \in U$ вида

$$u_t = U_t(y_0, ..., y_t, u_0, ..., u_t) ,$$

где U_t - некоторая детерминированная функция своих аргументов со значениями в R^N, зависящая (в общем случае) также и от текущего

времени t. Это уравнение, описывающее обратную связь, определяет реализуемые управления $\{u_t\}$ – при каждом t они могут зависеть только от предыстории процесса (прошлых значений выхода и управления), какое бы ни было само множество $U \subseteq R^N$.

Пусть y_t^o обозначает заданное значение выхода y_t одномерного объекта управления в момент t. Введем в рассмотрение некоторую неотрицательную скалярную функцию потерь $\tilde{\omega}(\varepsilon_t) \geq 0$, зависящую от текущей ошибки ε_t по выходу

$$e_t = y_t^o - y_t$$

и представляющую собой обычную четную функцию от ε_t:

$\tilde{\omega}(e_t) = \tilde{\omega}(-e_t)$.

Наиболее распространенными функциями потерь являются квадратичные $\tilde{\omega}(\varepsilon_t) = \varepsilon^2{}_t$ и модульные $\tilde{\omega}(\varepsilon_t) = |\varepsilon_t|$ функции от ε_t. Они являются так называемыми целевыми или оценочными функциями.

Известно, что локальный критерий качества J системы управления дает количественную оценку степени выполнения в момент t предписанных требований как некоторую операцию над функциями удельных потерь. В случае систем с нестохастическими возмущениями [4] локальным критерием качества будет следующий показатель:

$$J = \sup_{\omega:\varepsilon_i \leq \nu_i(\omega) \leq \varepsilon_s} \left| y_t^0 - y_t \right| .$$

Во многих случаях в практическом плане предпочтительнее оценивать качество работы системы управления некоторым функционалом J, определенным вдоль всей траектории движения системы. В частности, при работе в нестохастической среде можно ввести суммарный функционал относительно определенным образом выбранной функции удельных потерь:

$$J = \sum_{t=t_0}^{\infty} \tilde{\omega}(u_t, v_t) \quad ,$$

где:

u_t - вектор допустимых управлений;

v_t - вектор возмущений.

Для оценки качества работы систем управления применим критерий, который при $y_t^0 \neq 0$ можно записать так :

$$J = \left\| y_t^0 - y_t \right\| = \sup_{0 \leq t < \infty} \left| y_t^0 - y_t \right| . \quad (2)$$

Поскольку с течением времени система управления в принципе может повышать эффективность своего функционирования, более приемлемым критерием качества при наличии возмущения v_t является функционал, который характеризует предельные показатели качества управления:

$$J = \overline{\lim_{t\to\infty}} \left| y_t^o - y_t \right| .$$

В многосвязном объекте с N-мерным вектором выходных переменных $y_t = \left[y_t^{(1)}, ..., y_t^{(N)} \right]^T$, подверженному действию N-мерного вектора $v_t = \left[v_t^{(1)}, ..., v_t^{(N)} \right]^T$ неизмеряемых возмущений, критериями качества управления могут служить функционалы вида

$$J = \overline{\lim_{t\to\infty}} \left| y_t^{o(i)} - y_t^i \right|, \forall i = \overline{1, N} \quad ,$$

или

$$J = \overline{\lim_{t\to\infty}} \left\| y_t^{o(i)} - y_t^i \right\| \ , \forall i = \overline{1, N} \, ,$$

где $y_t^0 = \left[y_t^{0(1)}, ..., y_t^{0(N)} \right]^T$ – вектор заданных значений выходных переменных в момент t , а $\|\cdot\|$ обозначает евклидову норму вектора.

4. Особенности применения гиперкомплексных числовых систем при моделировании процессов в СУ ИС

Гиперкомплексная числовая система (ГЧС) - это алгебра над полем, которая одновременно является и кольцом и векторным пространством над заданным полем, причем выполняется ассоциативность умножения на скаляр и дистрибутивность умножения, как на вектор относительно сложения скаляров, так и на скаляр относительно сложения векторов [13].

Таким образом, каждую последовательность переменных в выражении (1) характеризующую процесс (действие) СУ ИС можно описать числом вида

$$A = a_1 e_1 + \ldots + a_i e_i + \ldots + a_n e_n = \sum_{i=1}^{n} a_i e_i, \quad (3)$$

и законом умножения базисных элементов

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ij}^k e_k \ , \quad (4)$$

где:

$a_i e_i$ – число, соответствующее определенному параметру;

$\{a_1,\ldots,a_i,\ldots,a_n\}$ – коэффициенты определяются системой чисел над которой задана ГЧС, и могут принадлежать вещественным, комплексным или другим гиперкомплексным числам;

$\{e_1,\ldots,e_i,\ldots,e_n\}$ – базис ГЧС, т.е. множество таких векторов в векторном пространстве, что любой вектор этого пространства может быть единственным образом представлен в виде линейной комбинации векторов из этого множества - базисных векторов;

γ_{ij}^k – структурные константы, которые являются вещественными числами: $\gamma_{ij}^k \in R$;

n – размерность векторного пространства.

Таким образом, при выходных переменных $Y = \sum_{i=1}^{N} a_i y_i$, критерий качества управления процессом (2) будет функционал от гиперкомплексных переменных

$$J = \left\| Y_t^0 - Y_t \right\| = \sup_{0 \le t < \infty} \left| Y_t^0 - Y_t \right| ,$$

где $Y^o = \sum_{i=1}^{N} a_i y_i^0$ – заданное значение выходных переменных в момент t, а $\|\cdot\|$ означает норму ГЧС.

Целью управления процессом СУ ИС является требование, которое налагается на необходимый показатель качества информационного сервиса. Следовательно, при управляющем воздействии

$$U = \sum_{i=1}^{N} b_i u_i$$

и заданном значении локального критерия качества информационной услуги

$$J^o = \inf_{U_t} j ,$$

выполнение следующих условий определяет цель управления:

- $J = J^0$ (оптимальность);
- $J \le J^0 + \delta$ для сколь угодно малого $\delta > 0$ (субоптимальность).

Согласно концепции реинжиниринга М.Хаммера [5], для описания процессов используются как методологии графических описаний (IDEF0, IDEF3, BPMN и т.д.), так и формальные подходы, основанные на применении графов, гиперграфов и метаграфов [6-10].

Переход от графического, полученного одним из средств автоматизированного проектирования систем, к гиперкомплексному

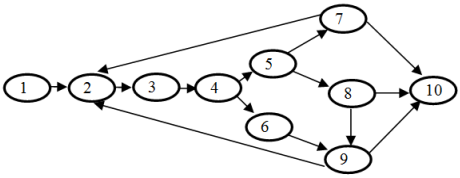
представлению информации о процессах СУ ИС, осуществляется в соответствии с нижеприведенными правилами.

1. Базис гиперкомплексные числовой системы образуется из точек схемы и необходимого количества путей. Причем, пути выбираются так, чтобы среди них не было линейно зависимых. Отсюда следует, что максимальная длина пути не может превышать n-1, где n - размерность гиперкомплексной числовой системы.
2. Точка граф-схемы – это путь нулевой длины.
3. Закон взаимодействия базисных элементов сводится к умножению путей, т.е. произведением путей является суммарный путь, если конец первого пути совпадает с началом второго пути. В противном случае произведение равно нулю.
4. Каждый элемент гиперкомплексные числовой системы является линейной комбинацией базисных элементов, которая обязательно включает все точки граф-схемы процесса.

В качестве примера применения данных правил, рассмотрим алгоритм информационного анализа естественных текстов с использованием метода графов горизонтальной видимости, описанного в [11].

1. Предварительная обработка текста: конвертация в нужный формат и регистр; выделение отдельных слов; стемминг.
2. Поиск уникальных лексических элементов текста .
3. Дисперсионная оценка важности лексических элементов текста.
4. Оценка весовых коэффициентов всех лексических элементов текста методом графов горизонтальной видимости;
5. Сортировка ассоциативного массива и фильтрация его по словарю стоп-слов (исключение стоп-слов для униграмм и биграмм).
6. Сортировка ассоциативного массива и фильтрация его по словарю стоп-слов (исключение или включение стоп-слов в состав N-грамм)
7. Выбор K наиболее информативных униграмм
8. Выбор L наиболее информативных биграмм (повторить п.п. 2-5)
9. Выбор T наиболее информативных триграмм и т.д. (повторить п.п. 2-4 и выполнить п.5)
10. Формирование корреляционной матрицы для N-грамм.

Построим граф-схему основных операции, которые осуществляются при исследовании естественных текстов: предобработке; построении антологии; расчете статистических показателей отдельных единиц информации; выделении наиболее характерных понятий (слов и словосочетаний).



Для краткости изложения будем считать, что каждая операция представляет собой ОУ с отрицательной обратной связью. Так же будем считать, что *i*-тая операция соответствует *i*-той переменной в формулах (3)-(4), а коэффициенты $a_2 \div a_6$ соответствуют количеству выполненных операций. Тогда гиперкомплексное представление данного процесса будет иметь следующий вид:

$$A = e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 + a_5 e_5 + a_6 e_6 + K e_7 + L e_8 + T e_9 + e_{10}$$

	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}
e_1	e_1	e_3-e_7-e_9	0	0	0	0	0	0	0	0
e_2	0	e_2	e_4	0	0	0	0	0	0	0
e_3	0	-e_1-e_7-e_9	e_3	e_5+ e_6	0	0	0	0	0	0
e_4	0	0	-e_2-e_7-e_9	e_4	e_7+ e_8	e_9	0	0	0	0
e_5	0	0	0	-e_3+ e_6	e_5	0	e_2+ e_{10}	e_9+ e_{10}	0	0
e_6	0	0	0	-e_3+ e_5	0	e_6	0	0	e_2+ e_{10}	0
e_7	-e_1+e_3-e_9	0	0	0	-e_4+ e_8	0	e_7	0	0	-e_8-e_9
e_8	0	0	0	0	e_7-e_4	0	0	e_8	-e_6-e_2-e_{10}	-e_7-e_9
e_9	0	-e_1+e_3-e_7	0	0	0	-e_4	0	-e_5+ e_{10}	e_9	-e_8-e_7
e_{10}	0	0	0	0	0	0	e_2-e_5	-e_5+ e_9	e_2-e_6	e_{10}

Необходимо отметить, что для эффективного использования ГЧС при моделировании процессов СУ ИС должны применяться такие алгебры, которые можно арифметизировать, то есть они должны содержать единичный элемент. Анализ результатов проведенных исследований показал, что этим свойством обладают ассоциативные алгебры над полем действительных чисел. [12-14] При их построении обычно применяют метод алгебры путей на графах. С его помощью можно строить конечномерные алгебры над полем действительных чисел путем первоначальной построения схемы алгебры с последующей генерацией таблицы умножения алгебры, которая соответствует приведенной выше схеме перехода.

Выводы

В работе был рассмотрен процессный подход к моделированию систем управления качеством информационных услуг. В качестве системы представления данных при моделировании СУ ИС, предложено использовать гиперкомплексные числовые системы. Данный подход позволит осуществить формальное описание параметров, ограничений и связей между ними, с учетом всей имеющейся информации, а также

известных законов, закономерностей и т.п., которые описывают процессы информационных сервисов.

Литература

1. Додонов А.Г. Компьютерные информационно-аналитические системы. Толковый словарь/ А.Г.Додонов, Д.В.Ланде, В.Г.Путятин.- К.: Наук.умка, 2011. – 384 с. ШИТ 978-966-00-1130-4

2. Quality management principles, ISO, 2001 - [Режим доступу: http://www.iso.org/iso/qmp_2012.pdf]

3. Словарь терминов ITIL версия 1.0, 29 июля 2011 г. Справочник технического переводчика./ – Интент. 2009-2013 - [Режим доступу: http://intent.gigatran.com/]

4. Балакришнан, А. В. Введение в теорию оптимизации в гильбертовом пространстве/ А. Балакришнан ; пер. Э. Л. Наппельбаум ; ред. Р. В. Гамкрелидзе. - М. : Мир, 1974. - 259 с.

5. Хаммер М., Чампи Д. Реинжиниринг корпорации. Манифест революции в бизнесе / – М.: Манн, Иванов и Фербер, 2011. – 288 с

6. Евгенев Г.Б. Интеллектуальные системы проектирования. – М.: МГТУ им. Н. Э. Баумана, 2009. – 336 с.

7. Дубейковский В.И. Эффективное моделирование с CA ERwin Process Modeler (BPwin; AllFusion Process Modeler) / – М,: "Диалог-МИФИ", 2009 – 384 с.

8. Мезенцев К.Н. Автоматизированные информационные системы. – М: Академия, 2014 – 176 с.

9. Basu A., Blanning R. Metagraphs and Their Applications. – New York: Springer, 2007. – 173 p.

10. Овчинников В.А. Графы в задачах анализа и синтеза структур сложных систем. – М.: МГТУ им. Н.Э.Баумана, 2014. – 424 с.

11. Ландэ Д.В., Снарский А.А., Безсуднов И.В. Интернетика: Навигация в сложных сетях: модели и алгоритмы - М.: Либроком (Editorial URSS), 2009. - 264 с. ISBN 978-5-397-00497-8

12. М.В.Синьков, Я.А. Калиновский, Т.В. Синькова, А.А. Чапор. О повышении производительности вычислений в некоторых классах гиперкомплексных числовых систем // Электронное моделирование, 2000. – № 6. – С. 13-18.

13. М.В. Синьков, Ю.Е. Бояринова, Я.А. Калиновский. Конечномерные гиперкомплексные числовые системы. Основы теории. Применения. – К.: ИПРИ НАН Украины, 2010. – 389 с. Я.А.Калиновский, Ю.Е.Бояринова. Высокоразмерные изоморфные гиперкомплексные системы и их применение. – К: ИПРИ НАН Украины, 2012. – 183с.

14. Калиновский Я.А., Ландэ Д.В., Бояринова Ю.Е., Хицко Я.В. Гиперкомплексные числовые системы и быстрые алгоритмы цифровой обработки информации. – К.: ИПРИ НАН Украины, 2013. – 125 с.

ВИКОРИСТАННЯ ГЕОГРАФІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З ВІДКРИТИМ КОДОМ ДЛЯ ВІДОБРАЖЕННЯ ТА ГЕОАНАЛІЗУ ІНФОРМАЦІЙНИХ ПОТОКІВ СИСТЕМ КОНТЕНТ-МОНІТОРИНГУ

Бріцький С.О., Ланде Д.В.
Інститут проблем реєстрації інформації НАН України

1. Постановка проблеми

Однією з вимог інформаційно-аналітичних служб на сьогодні є забезпечення їх засобами геопросторового аналізу інформаційних потоків різноманітного походження. В існуючих геоінформаційних системах (далі – ГІС) є можливість нанесення графічних позначок з текстовими мітками. Проте процес автоматичної прив'язки інформаційного повідомлення до точки на карті, а також відображення такої прив'язаної інформації засобами платформонезалежного веб-додатка на сьогодні потребує окремої реалізації.

2. Мета роботи

Запропонувати підхід до створення інформаційної автоматизованої системи відображення на географічній карті графічних посилань на інформаційні повідомлення, які можна об'єднувати в групи за належністю до точки на координатній площині.

3. Основні результати дослідження

Автором створено програмний модуль автоматичної географічної прив'язки інформації системи контент-моніторингу InfoStream до карти світу з відповідним її відображенням у вигляді графічних позначок та можливістю перегляду анотації/заголовку інформаційного повідомлення (групи інформаційних повідомлень) при натисканні мишкою на такі позначки.

Географічну частину системи реалізовано засобами програмного забезпечення з відкритим кодом OSGeo4W, Quantum GIS Server 2.0.1 (http://www.qgis.org), мови програмування PERL та системи управління базами даних Postgre SQL 9.3. Векторні шари у форматі SHP, растрові шари з прив'язкою до системи координат EPSG:4326-WGS84 взято з відкритих джерел мережі Інтернет.

Програмне забезпечення з відображення інформації у вигляді веб-додатка побудовано засобами OpenLayers 2.10 та PHP 5.2, які функціонують на базі веб-сервера Apache 2.0.

4. Висновки

Проведені дослідження дозволяють стверджувати, що на основі програмного забезпечення з відкритим кодом можливо побудувати систему

автоматичної географічної прив’язки структурованих інформаційних потоків на прикладі інформаційного масиву системи контент-моніторингу InfoStream. Очевидними перевагами такого підходу є низька вартість робіт та незалежність кінцевого програмного продукту від платформи клієнта, оскільки всі аналітичні операції відбуваються на боці сервера. При цьому слід зазначити, що географічна належність інформаційного повідомлення повинна бути визначена засобами системи контент-моніторингу.

До недоліків представленого підходу слід віднести те, що у разі відсутності попередньої географічної прив’язки інформаційного повідомлення слід провести таке визначення в інший програмний спосіб (або ж провести таку прив’язку вручну), а також необхідність побудови додаткових інструментів геопросторового аналізу порівняно з тими, які наразі присутні в комерційних ГІС.

ПЕРСПЕКТИВИ КРИМІНАЛІЗАЦІЇ СТАТТІ 173-1 КОДЕКСУ УКРАЇНИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

Верголяс О.О.
Національна академія СБ України

Постановка проблеми

В час масованої інформаційної атаки на свідомість людини та довготривалі кризові соціально-економічні та політичні явища, певна група людей мінімізує отримання інформації, інші – навпаки розширюють коло інформаційних джерел. Однак, як правило, коли суспільство входить в зону турбулентності, підвищення рівня соціальної напруги зменшується рівень довіри до органів державної влади а також до основних джерел інформації. На цьому фоні збільшується роль неформальних джерел отримання інформації, як то чутки. Як не дивно, однак саме чутки виходять на першу роль у кризових ситуаціях, коли особа не має доступу до інформації або самостійно обмежує для себе коло джерел інформації через недовіру до них. В залежності від ситуації, чутки можуть мати як істинну основу так і неправдиву, далі вже йде градація чуток за ступенем наявності достовірної інформації. Однак, як правило, серед суспільства превалюють чутки з негативним посилом. Поширення та ретрансляція чуток, які стосуються харчового забезпечення, соціальних виплат, курсу валют, поширення інфекційних захворювань, здійснення терористичних актів тощо, можуть викликати панічні настрої серед населення, які у свою чергу можуть вилитись у масові заворушення. На сьогоднішній день відповідальність за такого роду правопорушення передбачена статтею 173-1 Кодексу України про адміністративні правопорушення "Поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку» (далі ст. 173-1 КУпАП) [1]. На думку автора, здійснення такого правопорушення має каратись більш суворо, ніж один місяць виправних робіт, оскільки така діяльність несе за собою значну шкоду та загрозу безпеці та спокою суспільства.

Мета публікації

Аналіз та пропозиції стосовно криміналізації поширення неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку.

Аналіз останніх публікацій

Складність питання полягає у тому, що наявні наукові дослідження стосуються поширення неправдивої інформації у формі наклепу (обмови), поширення неправдивої (недостовірної) інформації –О. Кузнєцова, В.

Підгородницький, Н. Тимошенко, В. Вакулич та інші, та з іншого боку дослідження теми завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності – О. Кириченко, К.Берлянд, В. Навроцький, В. Тихий. Загалом питання чуток та їх поширення у суспільстві вивчали такі дослідники Л. Климанська, С. Зелинський, Л. Орбан-Лембрик, Г. Почепцов та інші.

Виклад основного матеріалу

Як видно з вищенаведеного, юридична думка виділяють такі форми розповсюдження неправдивої інформації, яка підлягає кримінальній відповідальності: завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності та поширення неправдивої інформації. Необхідно зазначити наступне, поширення неправдивої інформації (наклеп, обмова) є різновидом поширення неправдивих відомостей, які принижують честь та гідність особи. Зауважимо, що немайнові особисті (приватні) права осіб, якими є честь, гідність, репутація, відносяться до предмету регулювання цивільного права. Статтями 28 і 32 Конституції України [2], а також статтями 297 та 299 Цивільного кодексу України (далі – ЦК) [3] закріплюється право кожного на повагу до його гідності та честі, а також на недоторканість ділової репутації. При порушенні таких прав особа може звернутися до суду з позовом про захист гідності, честі та ділової репутації, які за статтею 201 ЦК відносяться до немайнових благ, що охороняються цивільним законодавством. Заподіяння моральної шкоди цим об’єктам цивільно-правової охорони шляхом розповсюдження недостовірних відомостей чи інформації підлягає відшкодуванню (стаття 23 ЦК). У цивільному законодавстві досить детально виписано механізм захисту немайнових благ особи, а тому всі, хто вважають, що на них було зведено наклеп, можуть скористатись його положеннями для свого захисту. Таким чином, цивільне законодавство забезпечує особі достатній захист у разі поширення неправдивої інформації про неї.

Крім того, поняття «наклеп», «образа», як і «честь», «гідність» та «ділова репутація» мають суб'єктивний індивідуально визначений характер. Відповідно й рішення про звернення до суду в цьому випадку має приймати особа, котра зазнала негативних наслідків від поширення завідомо неправдивих, недостовірних та негативних відомостей або інформації чи від образи.

З іншого боку, ст.259 Кримінального кодексу України чітко визначає коло інформації, яке може викликати паніку, а саме завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об’єктів власності [4]. Тлумачення даної статті та її застосування торкається лише повідомлення про замінування, тоді як поширення інформації стосовно, наприклад, отруєння джерел питної води під зазначену статтю не підпадають.

Загалом, як витікає із вище наведеного, статті як Цивільного кодексу так і Кримінального кодексів а також судова практика направлені проти або захисту честі, гідності та ділової репутації або неправдивої інформації стосовно підготовки до здійснення терористичного акту, в той же час ст. 173-1 КУпАП, з огляду на судову практику, фактично не працює, оскільки всі справи, що були у судовому розгляді стосувались поширення інформації про конкретну особу та наявність вибухового пристрою.

Для ґрунтовного підходу до питання наведемо визначення терміну «чутки».

Чутка — вістка, повідомлення про кого-, що-небудь, істинність якої не встановлено [5]. Чутки обертаються в соціумі, і мають неофіційний характер і передаються від особи до особи через приватне спілкування. Відповідно, якщо чутка була опублікована у ЗМІ або інших інформаційних джерелах то ця інформація перестає бути чуткою і отримує статус новинного повідомлення. Відповідно, при криміналізації ст. 173-1 КУпАП необхідно відокремити чутки як такі та інформацію, що поширюють ЗМІ та інші інформаційні джерела, що не зареєстровані як ЗМІ згідно до відповідного законодавства (блоги, сайти, популярні аканти у соціальних мережах тощо).

Паніка - один з найбільш помітних видів поведінки особи, маси (натовпу) і одночасно це особливий емоційний стан, що виникає як наслідок або дефіциту інформації про якусь лякаючу або незрозумілу ситуацію, або її надмірного надлишку, і що виявляється в стихійних імпульсивних діях [6]. Отже, як видно із визначення, паніка може бути як емоційним станом однієї особи так і кола осіб. Однак, виходячи з логіки правопорушення, а саме організації паніки серед населення, відповідно охоплення якомога ширшої аудиторії і підпадає під зазначену статтю.

Важливо відзначити, фабула зазначеної статті каже про чутки, що **можуть викликати паніку** серед населення. Відповідно, при використанні цієї статті постає питання у експертизі можливості провокування панічних настроїв серед населення, отже в процесі доведення вини мають бути залучені фахівці, які можуть довести що поширювана чутка може спровокувати паніку. Інше питання, коли паніка вже почалась, відповідно має бути покарання за чутки, що **викликали паніку серед** населення і тут постає питання не тільки у експертній оцінці чутки але й доведення, що саме ця інформація спровокувала паніку.

Звідси випливає перший аспект проблеми – **джерело поширення інформації та статус поширюваної інформації.** Відповідно, якщо працювати у напрямку криміналізації ст. 173-1 КУпАП необхідно опрацювати розділення інформаційних суб'єктів, а саме питання хто поширює інформацію і у який спосіб – фізична особа шляхом усної чи письмової розмови конфіденційно або у публічному місці, намагаючись привернути увагу оточуючих, чи ЗМІ та інші інформаційні джерела, що не зареєстровані як ЗМІ згідно до відповідного законодавства (блоги, сайти, популярні аканти у соціальних мережах тощо).

Іншим аспектом питання поширення чуток є наявність **кола осіб, організаторів, та суспільна небезпечність**, оскільки особа, що поширює чутку може бути як її ініціатором так і особою, що була введена в оману та хотіла попередити інших про наявну, з її точки зору, небезпеку і через певні суб'єктивні чи об'єктивні причини не повідомила правоохоронні чи інші компетентні органи про отриману інформацію.

У випадку, якщо особа або коло осіб **цілеспрямовано поширювали інформацію, усвідомлюючи її неправдивість**, необхідно застосовувати найбільш жорстку міру відповідальності. Організоване поширення чуток має на меті виклик панічних настроїв з метою отримання необхідного (для організаторів) результату як то збільшення попиту на товари першої необхідності, створення ажіотажного попиту на іноземну валюту, збільшення рівня недовіри до чинної влади та інші цілі, які можуть бути досягнені в результаті отримання панічних настроїв серед населення.

Особливо важливо звернути увагу на поширення чуток у зоні бойових дій, проведення антитерористичної операції, у зоні стихійного лиха, надзвичайної ситуації тощо, оскільки такі дії можуть негативно вплинути на організацію заходів антитерористичних сил, зашкодити заходам з евакуації населення, локалізації стихійного лиха та загалом посіяти паніку як серед населення, що знаходиться безпосередньо на зазначених та суміжних територіях так і загалом у інформаційному просторі, що може зашкодити інформаційній безпеці держави.

Інша ситуація, коли особа або коло осіб **поширюють недостовірну інформацію не усвідомлюючи її неправдивість**. У такому випадку варто обмежитись профілактичними та роз'яснювальними заходами. Варто зауважити, що до такого роду правопорушень схильні люди похилого віку, так наприклад часто такі ситуації трапляються із встановленням комунікаційних веж операторів стільникового зв'язку, коли особи похилого віку дізнавшись про встановлення зазначеного обладнання сприймають вікове погіршення власного здоров'я як результат роботи комунікаційного обладнання.

Разом з цим, варто взяти до уваги, що необхідно відокремити безпосередньо ініціатора (ініціаторів) та організатора (організаторів) поширення чуток від осіб, які виступають як випадкові розповсюджувачі інформації, відповідно розмежувати відповідальність та інструменти як профілактики так і покарання за поширення чуток.

Висновки

Отже, з огляду на вищенаведене можна зробити висновок про те, що питання перспективи криміналізації відповідальності за поширення чуток, неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку вимагає додаткового ґрунтовного дослідження та вивчення питань в суміжних галузях науки, як то соціальна психологія та юридична психологія. Окремо стоїть питання механізму

експертного доведення винуватості та її градації і, відповідно, міри покарання за вчинені дії.

Література

1. Верховна Рада УРСР. Кодекс України про адміністративні правопорушення [Електронний ресурс] / Верховна Рада УРСР – Режим доступу до ресурсу: http://zakon3.rada.gov.ua/laws/show/80731-10/print1443685042333355.
2. Верховна Рада України. Конституція України [Електронний ресурс] – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/print1443685187562867.
3. Цивільний кодекс України [Електронний ресурс] – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/laws/show/435-15/print1443686084026994.
4. Кримінальний кодекс України [Електронний ресурс] – Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/2341-14/print1443687078440915.
5. Словник української мови [Електронний ресурс] – Режим доступу до ресурсу: http://sum.in.ua/s/chutka.
6. Ольшанський Д.В. Психологія тероризму [Електронний ресурс] – Режим доступу до ресурсу: http://ibib.ltd.ua/panika-26455.html.

ДО ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ОРГАНІЗАЦІЇ УПРАВЛІННЯ ВИЩИМИ НАВЧАЛЬНИМИ ЗАКЛАДАМИ

Галушко М.М.[1], Самаріна М.О.[2], Ільницька Г.Т.[1]
[1]НТУУ «Київський політехнічний інститут»
[2] ДУ «Науково-методичний центр інформаційно-аналітичного забезпечення діяльності вищих навчальних закладів «Агроосвіта» МОН України

У сучасному світі рішення, що приймаються індивідом, багато в чому залежать від інформаційних технологій. Такі визначальні рішення (дії) в глобальному масштабі утворюють інформаційні мережі. У загальному і цілому, критерієм інформативності виступає ступінь насичення інформаційними технологіями тих чи інших видів людської діяльності. Цей критерій виступає в ролі визначального чинника розвиненості суспільства і економіки в цілому. Так як в сучасних умовах інформація, знання відіграють найважливішу роль у прийнятті навіть самих незначних рішень, це вимагає відповідного рівня підготовки фахівців, якісних змін у підготовці та перепідготовці кадрів, розвитку навичок, пов'язаних з обробкою величезних масивів інформації.

Відповідно, інформаційне суспільство, де основою розвитку стає не матеріальне виробництво, а виробництво знань та нематеріальних благ, відрізняється відкритою економікою, яка активно бере участь в процесах інтернаціоналізації і глобалізації; має високий рівень освіти і систему охорони здоров'я; розвинену конкурентоспроможну економіку та достатньо сильну інфраструктуру в області інформаційних технологій і виробництві знань.

Ближче всіх на шляху до інформаційного суспільства стоять країни з розвиненою інформаційною індустрією (США, Японія, Англія, Німеччина, країни Західної Європи). У цих країнах вже давно одним із напрямів державної політики є інвестиції та підтримка інновацій в інформаційній індустрії, розвитку комп'ютерних систем і телекомунікацій.

Як видно з досвіду таких країн, при переході від індустріального суспільства, направленого на виробництво і споживання товарів, в інформаційному суспільстві виникає індустрія переробки інформації на базі комп'ютерних і телекомунікаційних інформаційних технологій, коли більшість працюючих зайнято виробництвом, зберіганням, переробкою і реалізацією інформації, особливо вищої її форми - знань. Відповідно, одним із аспектів, що формують успішну соціалізацію особистостей, наразі стає соціальне виховання як складова системи функціонування вищих

навчальних закладів різних типів та галузевого спрямування. Загальною рисою при цьому стає формування соціально значущих якостей, сталих поглядів людини на природу, суспільство, продукти діяльності людини, на саму себе, певної системи мотивів, форм і способів поведінки, у яких ці погляди реалізуються [1, 2].

Крім «соціального наслідування», яке у вигляді мови, релігії, традицій і звичаїв, пам'яток літератури, результатів науки, всієї сукупності духовного змісту, накопиченого попередніми поколіннями як традиції, забезпечують вищі навчальні заклади при підготовці фахівців [3], необхідно переосмислювати інформаційний зміст та підходи до забезпечення як державної системи організаційного управління, так і такі підходи у вищих навчальних закладах, беручі до уваги нові нормативні вимоги та концептуальні парадигми.

Як специфічний регулятивний процес, організаційне управління, в тому числі й на етапі навчання молоді у вищих навчальних закладах та формування зрілих особистостей, покликано реалізувати соціально-економічний та культурний її потенціал, що залежить від організації процесу соціалізації молоді, оскільки саме молодь є стратегічним ресурсом держави завдяки високій життєвій активності, здатності до швидкоплинної адаптації та включення в суспільне життя.

Приклади зміни парадигми системи організаційного управління бачимо в підходах, запроваджених у аграрних вищих навчальних закладах 3-4 рівнів акредитації, коли для виміру рівня залишкових знань студентів запроваджено незалежне дистанційне оцінювання знань шляхом тестування. Наявне інформаційне забезпечення дає змогу оцінити й рівень адекватності фахівців вимогам сучасного виробництва, а також її соціалізації та стресостійкості.

Зміну парадигми у системі інформаційного забезпечення системи організаційного управління спостерігаємо на власному досвіді навчання у Комп’ютерній академії «Шаг», де викладачі навчають сучасним практичним знанням ІТ-індустрії.

Загальними рисами є наявність знань та нестандартне мислення, що є необхідним в сучасному організаційному управлінні, виробничих зв’язках між людьми, суспільному житті.

Подальше інформаційне забезпечення систем організаційного управління вбачаємо у розвитку регулюючого впливу на поведінку учасників спільної діяльності; соціального управлінні (координація, узгодження, планування, контроль, нагляд, примус), що можуть бути реалізовані в рамках суспільних відносин.

Література

1. Лобанова С. І. Сучасні підходи до визначення сутності поняття «соціальне виховання» / С. І. Лобанова // Збірник наукових статей Соціальна педагогіка: теорія та практика № 3, Луганськ: Луганський національний університет імені Тараса Шевченка, – 2010. – С.19-27.

2. Проект Етичного кодексу українського педагога [Ел. ресурс] – Електрон.дан. (1 файл). – Режим доступу: http://rmu.luguniv.edu.ua/img/ekup.pdf. – Заголовок з екрану.

3. Джур О. Б. Управління процесом виховання в сучасних умовах [Ел. ресурс] / О. Б. Джур – Електрон.дан. (1 файл). – Режим доступу: http://tme.umo.edu.ua/docs/Dod/2_2010/dzhur.pdf. – Заголовок з екрану.

ЗАКОНИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ФІЛОСОФСЬКО-АНТРОПОЛОГІЧНИЙ ВИМІР

Головко О. М.
НДІІП НАПрН України

У даний момент вирує дискусія стосовно майбутнього цивілізації, що заохочується в новій ситуації швидкого наукового й технічного поступу. Альфред Порт Вайтгед

Перед сучасною українською спільнотою в період загрози інформаційної безпеки нашої держави постало питання, що ж таке інформаційне суспільство: черговий міф для відволікання уваги від поточних соціально-економічних проблем чи реалії сьогодення, котрі перманентно впливають на суспільно-політичне життя не тільки України, а й усього світу?

У сучасному розумінні «інформаційне суспільство» – це передусім гуманітарна категорія, що описує якісні суспільні трансформації, зміщення акцентів із виробничої до невиробничої сфер, зміну характеру інформаційних потоків, групових та індивідуальних ідентичностей [3, с. 5].

З даного питання сьогодні активно ведуться дискусії філософами, соціологами, політологами та юристами. Різні аспекти інформаційного суспільства (далі – ІС) стали предметом широких громадських дискусій. Вони викликають не тільки загально філософський інтерес, але й стають надзвичайно важливими для вирішення нагальних практичних проблем.

У ході обговорення ідей і концепцій ІС будуються уявлення про особливості якісно оновленої системи суспільного устрою. В динамічному русі відбувається дослідження майбутніх механізмів влади та управління, формування та переосмислення цінностей в новітньому процесі життєдіяльності людини та суспільства тощо.

Науковці особливо акцентують увагу на масовому застосуванні всесвітньої мережі Інтернет. Так, наприклад, Баранов О.А. доречно зазначає, що треба особливо ретельно дослідити нові правові обставини функціонування засобів масової комунікацій в умовах широкого використання інформаційно-комунікаційних технологій, зокрема інтернет-технологій [1, с. 229].

Сьогодні дослідження законів функціонування ІС як явища, що створює передумови для формування нової парадигми людського світосприйняття стало сприйматися як нагальна потреба. Поступово про необхідність зміни підходів у теоретичному та практичному сенсі стає зрозумілим не тільки науковцям, а й правозахисникам, політикам, юристам-практикам, адже всі ми вже давно знаходимося у вимірі інформаційного суспільства.

Теоретичною основою дослідження стали праці та наукові тези філософів, соціологів та футурологів у сфері інформаційного права. У

науковому аналізі використовуються доробки таких науковців як Д. Дубов, І. Бачило, О. Соснін.

Основним напрямом дослідження людської спільноти в інформаційно-комунікативному вимірі найближчим часом, на нашу думку, є задоволення нагальної потреби більш чітко окреслити контури інформаційного суспільства як нового ступеня розвитку світового співтовариства.

Перехід до ІС, в якому інформація та знання виступають в якості основної соціальної цінності, означає радикальні зміни не тільки в суспільно-політичному, але й в економічному сенсі.

Правовідносини та правила поведінки у сфері розроблення й застосування високих технологій є проявом волі суспільства та забезпечуються прогресивними (інноваційними) заходами соціально-інформаційного впливу [2, с. 14].

Сутністю процесу формування глобальної системи ІС на нових цивілізаційних принципах децентралізації та оптимізації є становлення системи відкритого, індивідуалізованого суспільства, що створює сприятливі умови для безперервної освіти і самонавчання протягом усього життя людини. Так, інформатизація служить реалізації таких напрямів розвитку таких якостей особистості як компетентність у вузькопрофільних та широко профільних галузях, світогляд та творчість, оскільки забезпечує доступ до інформаційних ресурсів суспільства та надає ефективні засоби їх освоєння. Незважаючи на те, що прогрес ІС все більше асоціюється з володінням знаннями та інформацією, необхідно враховувати конкретні соціальні умови розвитку інформаційного суспільства в різних регіонах планети, а також психологічні та ідеологічні фактори, що піднімають роль інформації та знання в суспільній свідомості.

Основна ідея інформаційного суспільства у соціогуманітарному вимірі полягає у досягненні нової фази розвитку – «суспільства знань» і забезпечення для всіх рівного доступу до них [3, с. 3-4].

Вчені та науковці намагаються встановити, яке суспільство можна вважати інформаційним, що є його відмінними ознаками, які соціальні проблеми можуть бути вирішені і які соціальні цілі досягнуті при його побудові. На рівні окремих держав приймаються національні програми переходу до інформаційного суспільства. Зокрема, в Україні також існує така програма, яка була прийнята 09.01.2007, а саме «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки».

З цього можна дійти висновку, що з економічної точки зору індустріальне суспільство, де споживалися в основному товари перетворюється на суспільство, в якому основний ринок збуту займають послуги. Власне, в цьому й полягає основна суть переходу до ІС, оскільки інформація стає основним ресурсом. З цього випливає ряд особливостей в різних сферах, зокрема соціально-політичній та філософсько-правовій, де існуючі догми індустріального суспільства вже не спрацьовують.

Варто погодитись з думкою, що інституціональний розвиток засад інформаційного права відіграватиме дедалі більшу роль, найближчим часом воно стане повноцінною сферою права, яка відіграватиме визначальну роль у розвитку суспільства XXI століття, і наша юридична наука має бути до цього готовою [2, с. 14].

Однак, формування ІС ставить перед людством та всім цивілізованим світом велику кількість проблем технологічного, соціально-економічного і політико-правового характеру.

З доктринальної точки зору основними філософськими протиріччями інформатизації можна виділити такі:

- оптимізм з приводу включення індивіда в інформаційне середовище, незважаючи на небезпеку маніпуляції як індивідуальною, так і суспільною свідомістю;
- інтеграція в суспільстві та інформаційна нерівність;
- зростання можливостей для саморозвитку особистості і глибока криза духовності в інформаційному суспільстві;
- інформатизація як універсальний для всього людства шлях прогресу і неможливість побудови людством уніфікованого суспільства знань.

Зазначимо, що складні й динамічні процеси переходу до ІС безпосереднім чином позначаються на соціальній свідомості та правосвідомості. Враховуючи, які значні зміни відбуваються в українському комьюніті дослідження формування свідомості нових поколінь в інформаційному суспільстві є досить актуальним і ставить перед суспільством глобальні філософські питання.

Виходячи із вищезазначеного, можна виділити ряд характерних особливостей становлення інформаційної цивілізації. Ми вважаємо найбільш суттєвими наступні з них:

1. ІС притаманно, в першу чергу, формування умов для вирішення глобальних проблем людства, тобто в результаті передбачається забезпечення подальшого сталого розвитку людської цивілізації.

2. Способом взаємодії суспільства і природи на етапі становлення ІС є інтенсивно-еволюційний шлях сталого розвитку, що забезпечує подальшу безпеку цивілізації.

3. Постіндустріальному суспільству характерні наступні процеси: інформатизація свідомості, виховання, освіти, культури, моральності та права. У результаті реалізації цих процесів з'явиться нова людина, якій буде притаманна наявність пріоритету основних загальнолюдських цінностей.

4. ІС неможливо створити в окремо взятій країні, вирішення глобальних проблем під силу лише людству в цілому. У філософській доктрині вбачається, що на цьому етапі буде реалізований новий вид ненасильницької демократії, що дозволить кожній людині дійсно брати участь у прийнятті відповідальних рішень.

Власне, останній критерій означає можливість участі кожної людини в прийнятті глобальних рішень, що стосуються не стільки навіть національних

питань, скільки людства в цілому, актуальних питань в глобальному, планетарному масштабі.

Таким чином, більшість процесуальних проблем становлення та розвитку ІС не досліджені повністю, оскільки, по-перше, інформатизація тільки відбувається, можна сказати, знаходиться на початковому етапі; по-друге, динаміка постіндустріального суспільства настільки блискавична, що потребує постійного контролю, аналізу та невпинних досліджень як з боку науковців, так і з боку громадськості. При цьому ніхто не залишається осторонь суспільних процесів, що спричиняє інформатизація – в цьому й полягає основна сутність становлення інформаційного суспільства, котре ще називають постіндустріальним.

Література

1. Баранов О. А. Пріоритетні напрями розвитку інформаційного права в Україні / О. А. Баранов // Держава і право : Юридичні і політичні науки : Збірник наукових праць. – 2011. – Вип. 52 . – С. 225-231.

2. Бачило І., Соснін О. Інформаційне право як запорука інноваційного розвитку нації / Бачило І., Соснін О. // Віче. – 2012. – № 1. – с. 12-14.

3. Дубов Д.В. Інформаційне суспільство в Україні: глобальні виклики та національні можливості: аналіт. доп. / Д.В. Дубов, О.А. Ожеван, С.Л. Гнатюк. – К.: НІСД. – 2010. – 64 с.

ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ КОНТРОЛЮ ЗА ВИКОНАННЯМ ДЕРЖАВНИХ РІШЕНЬ

Гора О.Б.

Безумовно, проведення якісного контролю за виконанням державних рішень (ДР) неможливе без відповідного інформаційного-аналітичного забезпечення. Використання сучасних інформаційних технологій та засобів автоматизації для інформаційно-аналітичного забезпечення контролю за виконанням ДР дозволяє забезпечити вирішення на більш високому рівні завдань: інформаційної підтримки процесів підготовки та прийняття ДР; обліку прийнятих ДР та завдань, визначених у них; своєчасного збору, зберігання та обробки достовірної інформації щодо стану виконання ДР; моніторингу ходу реалізації ДР; аналізу зібраної інформації, виявлення відхилень від запланованих результатів та підготовки пропозицій щодо їх усунення; інформаційного забезпечення керівництва держави достовірною інформацією щодо стану виконання ДР.

Інформаційно-аналітична система контролю за виконанням державних рішень (ІАСК) є невід'ємною складовою частиною системи інформаційно-аналітичного забезпечення органів державного управління і призначена для забезпечення керівництва держави інформацією щодо стану реалізації ДР органами державної влади і місцевого самоврядування, установами та організаціями. Процеси інформаційної взаємодії у ІАСК можуть бути класифіковані наступним чином:

– обмін інформацією про стан виконання ДР між територіально-розподіленими структурами;

– отримання інформації від публічних інформаційних систем (насамперед з мережі Інтернет);

– опрацювання та аналіз зібраної інформації;

– підготовка експертних висновків про стан реалізації завдань, визначених у ДР, пропозицій щодо необхідності вжиття заходів реагування, інформаційно-аналітичних матеріалів для керівництва.

ІАСК повинна створюватися відповідно до основних принципів, дотримання яких є обов'язковим під час розробки інформаційно-аналітичних систем (ІАС). А саме: системності, гнучкості, технологічності в частині експлуатації та супроводу системи, надійності функціонування, ефективності використання елементів системи, стандартизації (уніфікації), забезпеченні можливості паралельного доступу до ресурсів системи, здатності до удосконалення та розвитку.

ІАСК – це сукупність розподілених баз даних і знань, інформаційних технологій, комп'ютерних систем, джерел і споживачів інформації, що об'єднані в одне ціле телекомунікаційними засобами і каналами зв'язку з метою вирішення загальних для системи завдань. У забезпеченні цільового призначення необхідно досягнути повної сумісності елементів системи,

узгодженості та збалансованості функціональних можливостей різних елементів системи. Саме модульна архітектура системи робить її гнучкою, здатною для подальшою її модернізації, тобто створює умови для зміни та налагодження на нові функціональні задачі. Цінність інформаційних ресурсів, результативність їхнього опрацювання, продуктивність інформаційної взаємодії насамперед залежать від вирішення питань організації доступу до інформаційних ресурсів, захисту інформації, систематизації різноманітної інформації і документів, узгодженості управління та представлення структурованих даних та неструктурованого "контенту" [1].

Важливим кроком реалізації системного підходу до моделювання ІАСК є визначення переліку типових завдань і функцій, які має виконувати зазначена ІАС. Предметна область, що досліджується, поєднує у собі риси різних галузей знань. Тому за результатами проведеного дослідження до основних завдань ІАСК можна віднести:

1) планування роботи з підготовки ДР;
2) контроль за ходом опрацювання проектів ДР;
3) моніторинг діяльності міжвідомчих комісій (робочих груп), створених для підготовки та моніторингу виконання ДР;
4) облік ДР, а також конкретних завдань, визначених у них, що підлягають контролю;
5) оперативний контроль за своєчасністю надання виконавцями звітної інформації, моніторинг ходу реалізації поставлених на контроль завдань;
6) моніторинг ЗМІ, Інтернету, статистичної та відомчої інформації на предмет наявності корисної для оцінки стану виконання завдань інформації;
7) збір, опрацювання та групування звітної й додаткової інформації відповідно до прийнятих ДР та завдань, визначених у них;
8) аналіз отриманих даних на предмет їхньої відповідності запланованим результатам, виявлення відхилень реальних результатів від запланованих і виявлення порушень, що були допущені в ході виконання ДР, та внесення пропозицій щодо вжиття заходів з їх усунення;
9) підготовка відповідних аналітичних матеріалів, довідок, звітів про стан виконання ДР.

До складу ІАСК повинні входити структурні компоненти та функціональні підсистеми. Структурними компонентами системи є: центральна підсистема ІАСК та функціональні вузли в органах державної влади, які забезпечують реалізацію ДР. Розподілені комп'ютерні системи є системоутворюючою складовою сучасних інформаційних інфраструктур. Комп'ютерні технології забезпечують інформаційну інтегрованість при наявній географічній розподіленості [2].

Центральна підсистема ІАСК призначена для отримання інформаційних матеріалів від інших складових системи, їх зберігання, аналізу та

узагальнення. Центральна частина ІАСК може складатися із двох фізично роз'єднаних локальних обчислювальних мереж:

– внутрішня локальна обчислювальна мережа – забезпечує доступ експертів (користувачів системи) до інформаційних ресурсів ІАСК;

– зовнішня локальна обчислювальна мережа – забезпечує доступ експертів до мережі Internet, інформаційних центрів, бібліотек, баз даних та зв'язок з державними органами – виконавцями ДР.

Функціональні вузли ІАСК в органах державної влади, інших установах і організаціях забезпечують формування інформаційних повідомлень для центральної підсистеми, на основі даних про хід реалізації ДР, які є у їхньому розпорядженні. Кожна підсистема центральної частини ІАСК складається із функціональних АРМів, які забезпечують вирішення визначеного комплексу задач. До того ж для розв'язання конкретних задач, АРМи інформаційно взаємодіють між собою за допомогою засобів мережі.

Рис. 1. Структурно-функціональна схема центральної частини ІАСК

Структурно-функціональна схема центральної частини ІАСК наведена на рис. 1. Кожна із вказаних підсистем тісно зв'язана із функціональними завданнями ***підсистеми контролю за виконанням ДР***.

Робота із забезпечення контролю за виконанням ДР повинна розпочинатися з етапу підготовки проектів самих ДР, оскільки від якісної підготовки відповідних проектів, системності завдань, визначених у них, залежать кінцеві результати їх виконання. Саме для цього призначені *підсистема планування роботи з підготовки ДР* і *підсистема підготовки проектів ДР та контролю за ходом їх опрацювання і узгодження*.

Для підготовки проектів ДР та у ході контролю за їх виконанням можуть створюватися різноманітні міжвідомчі робочі групи, проводиться наради та "круглі столи". Зазначені заходи проводяться згідно із завданнями,

визначеними у внутрішніх розпорядчих документах. Контроль за їх виконанням здійснюється за допомогою *підсистеми контролю за діяльністю міжвідомчих комісій (робочих груп)* та *підсистеми контролю за виконанням внутрішніх розпорядчих документів (внутрішній контроль)* і також безпосередньо пов'язаний з контролем за реалізацією ДР (зовнішній контроль).

Підсистема взаємодії із зовнішнім інформаційним середовищем. Ефективність отримання та опрацювання інформації у ІАСК багато в чому визначає ефективність роботи всієї системи контролю. Тому нагальною є необхідність забезпечення відповідного інформаційного обміну між центром прийняття ДР та органами державної влади – виконавцями завдань.

Первинна інформація щодо стану виконання ДР надсилається відповідними органами державної влади, підприємствами і установами, визначеними виконавцями ДР. Крім того, додаткова інформація може також надходити із ЗМІ, інформаційних ресурсів, від громадських організацій та громадян.

Водночас, збір, узагальнення та аналіз інформації це лише частина роботи із забезпечення контролю за виконанням ДР. Для прийняття обґрунтованих рішень щодо вжиття заходів реагування необхідно зібрану інформацію представити у зручному для сприйняття вигляді. Саме для цього призначена *підсистема виведення та візуалізації інформації*, за допомогою засобів якої інформація виводиться у вигляді таблиць, діаграм, графіків тощо.

Підсистема документообігу обслуговує усі інші підсистеми. Зокрема технологія збору та накопичення інформації в ІАСК передбачає її одноразове введення, формалізацію передачі під час інформаційного обміну між структурними компонентами, а також необхідну і допустиму, з урахуванням рівня доступу, інтеграцію як в межах усієї системи, так і в межах окремих функціональних підсистем.

Інформаційні ресурси ІАСК мають формуватися на основі регулярних регламентних звітів про стан виконання ДР та ручного введення даних. Основним засобом поповнення та оновлення інформаційних ресурсів має стати автоматизоване отримання, перевірка та зберігання даних. Ручне введення може використовуватися лише у тому випадку, коли відсутній електронний носій ресурсу.

Підсистема адміністрування та захисту інформації забезпечує ведення списку користувачів системи, надання їм прав доступу до інформації та складових підсистем у залежності від функціональних обов'язків користувача, захист інформації від стороннього втручання, резервне копіювання даних тощо.

В ІАСК інформаційна безпека та захист інформації набувають особливої ваги, враховуючи високий державний статус інформації, що обробляється. Проблема забезпечення інформаційної безпеки ІАС є комплексною і для її розв'язку необхідно поєднання як програмно-технічних заходів, що

запобігають або ускладнюють несанкціонований доступ до елементів мережі та до інформації, так і адміністративно-організаційних, спрямованих на створення належних умов безпечного функціонування та користування ІАС [3].

На сьогодні, захист інформації досить розвинута галузь науки і техніки, що пропонує на ринку широкий спектр різноманітних засобів для захисту інформації. Проте жоден з них окремо взятий не в змозі гарантувати адекватну безпеку ІАС. Надійний захист можливий лише за умови проведення комплексу взаємодоповнюючих заходів, серед яких можна виділити наступні: нормативно-правові засоби; адміністративні заходи; спеціальне обладнання і програмне забезпечення.

Враховуючи зазначене, для вирішення визначених задач ІАСК повинна об'єднувати комплекс нормативно-правового, технічного та організаційно-методичного забезпечення (рис. 2).

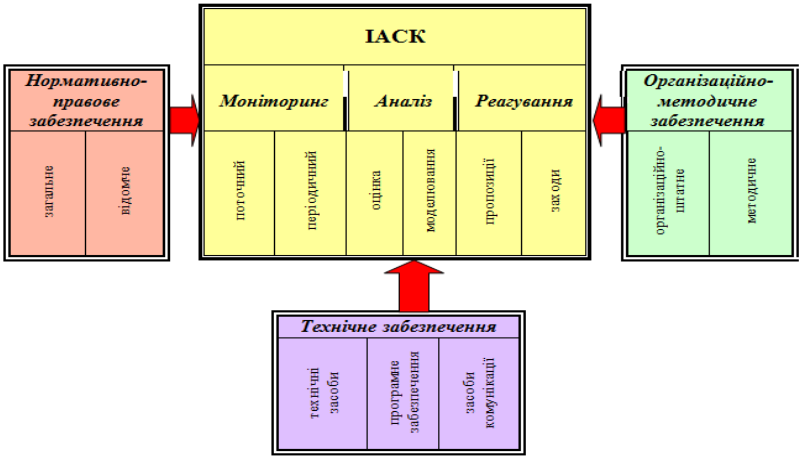


Рис. 2. Схема забезпечення вирішення задач ІАСК.

Нормативно-правове забезпечення ІАСК можна розділити на:

– загальне – нормативно-правові акти з питань організації та здійснення контролю за виконанням ДР, функціонування ІАС та захисту інформації, які поширюють свою дію на всі державні і недержавні установи та організації;

– відомче – нормативні акти державних установ, прийняті з метою забезпечення виконання ДР, функціонування ІАСК та захисту інформації в них.

Організаційно-методичне забезпечення складається з:

– організаційно-штатного – у державних органах повинні бути структурні підрозділи з питань організації та здійснення контролю за виконанням ДР, підтримки функціонування ІАСК та захисту інформації в них;

– методичного – це різного роду інструкції, методичні рекомендації, настанови з організації та здійснення контролю за виконанням ДР, функціонування ІАСК, захисту інформації тощо.

Технічне забезпечення ІАСК складається з технічних засобів (ПЕОМ, сервери, принтери, сканери і т.ін.), програмного забезпечення (Windows, SQL-Server, OPTiMA-WorkFlow, FineReader тощо), засобів комунікації (локальні мережі, Internet, Національна система конфіденційного зв'язку) та комплексних систем захисту інформації.

Загалом впровадженням ІАСК на основі наведеної моделі можна досягти наступних результатів:

- підвищити оперативність опрацювання інформації про стан виконання ДР;
- ппідвищити обґрунтованість і якість оцінки стану виконання ДР;
- ппідвищити якість контролю за виконанням ДР та результативність їх виконання.

Література

1. Горбачик О.С. Організація корпоративної аналітичної діяльності та сучасні технології її підтримки / О.С. Горбачик // Реєстрація, зберігання і обробка даних. – 2006. – № 3. – С. 32-39.

2. Горбулін В.П. Розподілені комп'ютерні системи як складові інформаційних інфраструктур / В.П. Горбулін, О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова // Реєстрація, зберігання і обробка даних. – 2008. – № 4. – С. 19-24.

3. Додонов О.Г Архітектура автоматизованих інформаційно-аналітичних систем органів державної влади / О.Г. Додонов, О.В. Нестеренко, М.М. Будько // Математичні машини і системи. – 2003. – № 3,4. – С. 138-146.

МЕТОДОЛОГІЧНІ ОСОБЛИВОСТІ МОДЕЛЮВАННЯ СОЦІОТЕХНІЧНИХ СИСТЕМАХ

Горбачик О.С.
Інститут проблем реєстрації інформації НАН України

Важливою рисою сучасності є залежність основних сфер життя суспільства від ефективного застосування інформаційних та комунікаційних технологій. Поширення цих технологій привело до появи складних системних утворень, що поєднують техніко-технологічні та соціальні системи, – соціотехнічних систем (СТС). Незважаючи на широке коло досліджень, треба констатувати, що стосовно соціотехнічних систем нині недостатньо опрацьовані теоретико-методологічні питання, аспекти практичного впровадження, питання безпеки їх функціонування, розвитку та взаємодії СТС. Можливо це пов'язано з тим, що більшість досліджень проводяться з позицій забезпечення стійкого функціонування СТС, а не розвитку системи, у той час, як постійний розвиток компонент СТС став умовою її існування. Розвитку технічної і технологічної компонент СТС вимагають умови ділового середовища, постійно зростаюча технологічна конкуренція, періодичне оновлення технічних засобів. Соціальна складова СТС включає досить специфічні активи (інтелектуальні і ділові якості співробітників, кваліфікацію керівного складу, корпоративний досвід тощо), які характеризуються відсутністю відчутної форми, довгостроковістю застосування, і також мають властивість приносити дохід лише у разі перманентного якісного розвитку. Отже, розвиток є однією із визначальних особливостей СТС, яка сприяє її якісним змінам, і це має враховуватися методологією досліджень.

Особливий компонентний склад СТС призводить до появи значного системного ефекту, який і надає переваги й можливість реалізації визначеної цілі функціонування. Компоненти поєднуються в СТС заради системного ефекту (емержентності) – виникнення певних властивостей, що роблять можливим досягнення цілей, які недосяжні для окремих компонентів СТС поза системою.

Як зазначається в [1], чим сильніше виражений системний ефект, тим частіше змушені говорити про притаманну системі складність. СТС є складною системою, що характеризується багатогранністю процесів управління, поганою прогнозованістю, інтенсивною взаємодією із зовнішнім середовищем та складністю внутрішньосистемного обміну. Завдання, що вирішуються засобами СТС, також, як правило, характеризуються складністю, суперечливістю вимог, неточністю формулювань.

З точки зору організаційно-управлінських процесів та фізичної організації СТС можна охарактеризувати як функціонально визначену структурно впорядковану з можливістю адаптивної реорганізації множину

елементів, до складу якої входить соціальна група, пов'язана цільовими зобов'язаннями, і технічна система, з використанням засобів якої досягаються загальносистемні цілі [1]. Зовнішні та внутрішні функції СТС можна характеризувати відповідними процесами інформаційної взаємодії та обмінними потоками. Адаптивна організація з активними механізмами реконструкції, реконфігурації й реорганізації є визначальною для існування СТС.

Функціонування СТС характеризується [2,3] активністю (СТС не лише реагує на зовнішні впливи, але й взаємодіє з середовищем); гомеостазом стану (СТС таким чином взаємодіє з середовищем, що забезпечується підтримання істотних змінних системи у припустимих межах на рівні, достатньому для самозбереження системи); функціональним гомеостазом (СТС таким чином взаємодіє з середовищем, що підтримується стабільне функціонування системи); автономністю (СТС містить сукупність автономних у системному розумінні підсистем); ієрархічністю (СТС структурно утворена у формі просторово-часової ієрархії функціональних систем); домінантністю (загальна спрямованість функціонування СТС при одночасному формуванні декількох цілей у кожний момент часу визначається по домінуючій цілі); цілісністю (кожній цілісній функціональній системі властива у просторі й часі своя адекватна область існування); перманентним розвитком (кожна цілісна функціональна система перманентно спрямована до максимізації у просторі й часі адекватної області свого існування).

Зазначене вище змушує говорити про необхідність спеціальних підходів до моделювання СТС, які б дозволяли з'ясувати залежності якості функціонування СТС від параметрів системи і зовнішнього середовища, структури, ієрархії функцій, алгоритмів взаємодії елементів.

Користуючись методологією системного аналізу, для дослідження структури СТС, функціонування (траєкторії СТС у просторі станів), забезпечення необхідної точності, врахування множини суттєвих характеристик доцільно робити багаторівневий опис СТС [3]. Наприклад [1], зробити інформаційний опис СТС, у якому визначити інформаційні зв'язки системи із зовнішнім середовищем, правила отримання і обробки інформації; функціональний опис СТС – окреслити множину функціональних елементів СТС і відношень між ними; технічний опис – визначити технічну структуру системи із відповідними засобами. Враховуючи, що СТС створюються заради отримання суттєвого системного ефекту, такий об'єкт дослідження має бути змодельований і як нероздільна сукупність дій, правил, методологій, принципово необхідних для існування системи і цілеспрямованого ефективного функціонування.

Дослідити СТС на цільовому рівні можна, застосовуючи методологію проектного менеджменту, що спирається на концепцію діяльності і результатів. СТС визначається як складна система $\mathfrak{I}$:

$$\Im = \langle Obj, Str, Tech, Fct, U \rangle,$$

де $Obj = \{obj\}$ – сукупність цілей; $Str = \{Str_{орг}, Str_{соц}, Str_{інф}, Str_{тех}, ...\}$ – сукупність структур, реалізуючих цілі (організаційна, соціальна, інформаційна, технічна тощо); $Tech = \{meth, proc, means, al\}$ – сукупність технологій (методи, методики, ресурси, алгоритм); $Fct = \{F_{ex}, F_{in}\}$ – фактори, що впливають на функціонування; U – процес функціонування.

Сукупність моделей СТС все одно лишається спрощеним відбиттям реального об'єкта, але надає можливість зробити певні теоретичні узагальнення, дослідити особливості причинно-наслідкових відношень, притаманних СТС, зафіксувати у явному вигляді притаманні їм закономірності, зв'язки і відношення, враховуючи при цьому їх ймовірнісну природу, дослідити вплив випадкових факторів на хід процесів у СТС, надаючи можливості для безпосереднього аналізу і змістовної інтерпретації результатів.

Література

1. Чимшир В.И. Сложность как граница управляемости сложной социотехнической системой //Сборник научных трудов «Вестник НТУ «ХПИ» «Нові рішення в сучасних технологіях», 2011. – №43. – С.101– 105.

2. Белецкая Л.В. Информационные технологии в бизнесе. Ч.1. / Л.В. Белецкая, В.П. Киреенко, Н.Н. Послов; под ред.. Т.В. Борздовой. – Минск: ГИУСТ БГУ, 2012. – 86с.

3. Додонов О.Г. Комп'ютерні засоби й інформаційні технології підтримки процесів управління реалізацією ділових процесів / Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. // Реєстрація, зберігання і обробка даних: зб. наук. праць за матеріалами Щорічної підсумкової наукової конференції 14-15 травня 2014 / НАН України. Інститут проблем реєстрації інформації, відпов. ред. В.В. Петров. – К.: ІПРІ НАН України, 2014. – С.54-58.

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ВІТЧИЗНЯНОГО МЕДІА-ПРОСТОРУ З МЕТОЮ ПОШИРЕННЯ СЕПАРАТИСТСЬКОЇ ІДЕОЛОГІЇ В УМОВАХ ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ НА СХОДІ УКРАЇНИ

Гребенюк М.В.
Національна академія Служби безпеки України

Підконтрольні керівництву РФ та «ДНР-ЛНР» медіа та Інтернет-ресурси продовжують нарощувати інформаційний тиск на Україну шляхом підготовки тенденційних матеріалів направлених на дискредитацію української держави, правоохоронних органів та командування Збройних Сил України, висунення звинувачень у невиконанні «Мінських домовленостей», послаблення міжнародної підтримки України, позитивного висвітлення діяльності керівництва «ДНР-ЛНР». За вказівки спецслужб РФ, російські ЗМІ та мас-медіа «ДНР-ЛНР», шляхом отримання акредитації в зоні проведення АТО для проведення зйомок на територіях, підконтрольних ЗС України, мають наміри підготувати низку компрометуючих матеріалів про діяльність українських добровольчих батальйонів «Азов», «Айдар», «Донбас» тощо.

«В.о. міністра інформації ДНР» М. Бережньовою у серпні 2015 року було доручено підконтрольним інформаційним ресурсам створити цикл відеосюжетів, що посилюватимуть ілюзію фінансової незалежності «ДНР». Опубліковані матеріали планувалося використати у «республіканських» інформаційних ресурсах та провідних ЗМІ РФ для підвищення рівня ненависті до населення України, недопущення виникнення ідеї повернення тимчасово окупованих територій під контроль нашої держави.

Керівником інформагентства РФ «Anna-news» А.Влаєвою отримано вказівку від російських «кураторів» щодо необхідності створення серії інформаційних повідомлень з метою легалізації отримання НЗФ «ДНР-ЛНР» зброї з РФ. За задумом, у зазначених матеріалах висвітлюватиметься фальсифікована інформація про викриття представниками «республіканських» збройних формувань схованок «невстановленої» зброї, яка буде вилучена та в подальшому використовуватиметься у бойових діях. Для підтвердження цих фактів планувалося проведення офіційних інтерв'ю та прес-конференцій з представниками «МГБ ДНР».

Непоодинокі випадки діяльності на території т.зв. «сірої» зони (знаходяться між 1 та 2 лінією зіткнень) окремих іноземних журналістів та представників проросійських громадських організацій без будь-яких дозвільних документів військового командування АТО, які готують репортажі з метою дискредитації сил АТО.

Зокрема, у «сірій» зоні здійснюють свою діяльність окремі громадяни РФ, представники т.зв. проросійських організацій «Российский мемориал», «Международная організація защиты прав человека», які під виглядом

надання гуманітарної допомоги, вивчення гуманітарної ситуації району займаються збором та фіксацією інформації щодо місць дислокації, переміщень та планів військових сил АТО. Водночас, вказані громадські організації активно співпрацюють з проросійськи налаштованими журналістами іноземних ЗМІ (фрілансерами), які згодом використовують здобуті відомості для підготовки та оприлюднення викривлених, тенденційних матеріалів на інформаційних ресурсах російських ЗМІ, в яких обвинувачується чинна влада України у створенні умов погіршення гуманітарної ситуації в зоні проведення АТО тощо.

У «ДНР-ЛНР» продовжуються заходи із створення власних телекомунікаційних мереж. Згідно наказу глави «ДНР» О.Захарченка, з 10.07.2015 замість мобільних операторів «МТС» та «Life» на території «республіки» працюватиме GSM-оператор «Фенікс», який з 01.06.2015 вже функціонує на території «ЛНР». У мережі оператора стільникового зв'язку «Фенікс» перебуває приблизно 7000 абонентів (усього до тестової експлуатації передано понад 9 тис. сім-карт), а сім-карти є у вільному продажу у відділеннях «Пошти Донбасу». Зона покриття оператора «Фенікс» складає 75% території «ДНР», у зв'язку з чим було введено в експлуатацію більше 270 базових станцій, прокладено близько 40 км нової оптоволоконної лінії зв'язку. При цьому у будівництві оператора стільникового зв'язку використовувалися OpenSource технології, а саме «OpenSwitch» та «OpenSS7», «The 3Gdb Home Subscriber Server». Розташована штаб-квартира оператора «Фенікс» у м. Донецьку, в колишній адмінбудівлі з використанням потужностей «Київстару». За діяльність «Феніксу» відповідає представник Міністерства зв'язку «ДНР».

Керівництвом «ДНР» надано вказівку «апарату глави республіки», посадовцям, військовому керівництву та військовим формуванням найближчим часом припинити використання сім-карток українських операторів та використовувати лише картки оператора «Фенікс» для зменшення ризику витоку «конфіденційної інформації». Послуги зазначеного оператора надаються всім бажаючим, вартість стартового пакету складає 100 грн. Для реєстрації абонента обов'язковою умовою є надання ксерокопії свого паспорту. Особливістю вказаної мережі є відсутність можливості здійснювати вихідні та вхідні дзвінки на номери інших мобільних операторів.

Російськими кураторами до мм. Донецька та Луганська для підрозділів, відповідальних за інформаційно-пропагандистську діяльність «ДНР-ЛНР» у серпні 2015 року було завезено технічне обладнання (великі телевізори з ширококутними камерами високороздільної чіткості та інші технічні засоби) з метою організації телемостів між самопроголошеними республіками.

З території м. Стаханова Луганської області здійснює мовлення радіостанція «ЛНР» «Казачье радио Всевеликого Войска Донского» на хвилі 102,5 FM. Можливості передавача дозволяють транслювати зазначену радіостанцію вглиб території підконтрольній Україні. Інформація, що

подається, викривляє реальні події, що відбуваються в Україні, а також сприяє формуванню у аудиторії слухачів настроїв спрямованих на підтримку та розвиток ідеї створення і функціонування «ДНР-ЛНР».

Додатковим механізмом розповсюдження сепаратистської ідеології та підтримки діяльності терористичних організацій на території України служать електронні засоби соціального зв'язку, які активно використовуються проросійськими структурами внаслідок їх обмеженої контрольованості з боку правоохоронних органів. Владні круги «республік» продовжують реалізовувати інформаційну незалежність від Києва та сприяють безперешкодному обміну інформацією інтернет-провайдерами та операторами зв'язку «ДНР-ЛНР». Співробітниками Краснодонського відділу «МДБ ЛНР» (м. Краснодон Луганської області) здійснюється тиск на керівництво інтернет-провайдеру «IP-COM» з метою подальшого контролю за трафіком абонентів.

Керівництво «Національної ради з питань телебачення і радіомовлення ДНР» має наміри задіяти передавачі на території РФ для трансляції сигналу аналогового мовлення телеканалів «ДНР» і Росії на територію м. Маріуполя та прилеглих населених пунктів, використовуючи таку сприятливу обставину, як відсутність природних перешкод. Зокрема, планується задіяти можливостей РТПЦ у м. Таганрозі (передавач потужністю 5 кВт) або м.Єйську (1 кВт). У «ДНР» оголосили про розширення покриття цифровим телебаченням території від м. Краматорська до Волновахи (близько 110 км) для трансляції російських та 4 каналів «ДНР». Канали не зашифровані та доступні без обмежень.

В інформаційній сфері сепаратистами забезпечується домінування російських телемовників (канали «*ОРТ*», «*LifeNews*», «*Россия 24*», «*НТВ*», ін.) та власного інформаційного продукту з одночасним блокуванням українських ЗМІ.

На тимчасово окупованих територіях продовжується процес формування власних підконтрольних медіа-ресурсів. Зокрема, у найбільших містах «ДНР» заплановано запуск цифрового телебачення, спочатку у великих містах, де діє велика кількість аналогових каналів та розвинуте кабельне телебачення, а згодом і у інших населених пунктах.

За розпорядженням кураторів з Управління ФСБ РФ у Ростовській області, співробітниками «МДБ ДНР» планується посилення інформаційної роботи як в «ДНР-ЛНР», так і на території, контрольованій Україною, шляхом проведення спеціальних інформаційних операцій.

Таким чином, аналіз ситуації у інформаційному просторі вказує на продовження здійснення представниками російських медіа структур та підконтрольних ним сепаратистських центрів «ЛНР-ДНР» агресивних заходів, спрямованих на:

- нагнітання негативного інформаційного фону довкола ситуації в зоні АТО та необхідності надання РФ гуманітарної допомоги;
- дискредитацію української державності, формування іміджу

України як країни, в якій на державному рівні пропагується фашистська (нацистська) ідеологія;

- звинувачення української влади та сил АТО в порушенні норм міжнародного гуманітарного права та «Мінських домовленостей», що призводить до чисельних жертв серед місцевого населення; дискредитацію можливостей Збройних Сил України з протистояння зовнішнім загрозам та здатністю надавати опір силам самопроголошених республік;
- провокування невдоволеності серед українського населення та ЗС України політикою української влади; створення умов для легітимізації влади «ДНР» і «ЛНР»;
- формування суспільної свідомості і громадської думки у вигідному сусідній державі-агресору ракурсі, в т.ч. через проведення спеціальних інформаційних операцій.

ПРАВОВІ ПИТАННЯ РОЗМЕЖУВАННЯ ЮРИСДИКЦІЙ В МІЖНАРОДНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Грицун О.О.
Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка

Перш за все, хочеться звернути увагу на те, що переважна більшість міжнародно-правових документів, що регулюють ті чи інші аспекти міжнародної інформаційної безпеки, взагалі не містять положень стосовно визначення юрисдикції в інформаційному просторі. Зокрема, в Угоді між урядами держав-членів Шанхайської організації співробітництва щодо співпраці у сфері забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року йдеться лише про те, що «держави-учасниці здійснюють співробітництво в міжнародному інформаційному просторі таким чином, щоб сприяти соціальному та економічному розвитку, у відповідності із завданнями підтримки міжнародної безпеки та стабільності, відповідати загальновизнаним принципам і нормам міжнародного права, включаючи принцип мирного врегулювання спорів, незастосування сили, невтручання у внутрішні справи держави, поваги прав та свобод людини, принципи регіонального співробітництва та невтручання в інформаційні ресурси держав-учасниць» [1]. Основними формами та механізмами співробітництва, відповідно до положень вищезазначеної угоди визнано: визначення компетентних органів держав-учасниць, відповідальних за виконання положень угоди; створення каналів прямого обміну інформацією щодо напрямків співробітництва; проведення консультацій уповноважених представників та компетентних органів, а також укладення договорів міжвідомчого характеру [1]. Таким чином, жодної статті чи положення, що регулювали б питання юрисдикції в Угоді держав-членів ШОС ми не знаходимо.

Схожа ситуація прослідковується і в Угоді про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі із злочинами у сфері комп'ютерної інформації від 01 червня 2001 року та в проекті Угоди про співробітництво держав-учасниць Співдружності Незалежних Держав у сфері забезпечення інформаційної безпеки. Як і в попередньому документі ці угоди визначають лише механізми співробітництва у формі: обміну запитами про надання сприяння, обміну інформацією, створення уповноважених органів, реалізації міждержавних програм та інших механізмів, оминаючи питання визначення юрисдикції в міжнародному інформаційному просторі.

Питання розмежування юрисдикцій частково висвітлено у Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року, проте питання ще далеке від вирішення з таких причин: порівняно невелика кількість держав є учасниками зазначеної конвенції; положення конвенції

орієнтовані скоріше на заходи співробітництва, тому питання визначення юрисдикції в кінцевому випадку залишаються на розгляд держав; держави можуть відмовитись від співробітництва, посилаючись на політичну винятковість ситуації; обов'язковою умовою для держав є лише проведення консультацій щодо визначення юрисдикції.

В Конвенції Ради Європи питання визначення юрисдикції врегульовано наступним чином: держава вживає необхідних заходів для встановлення юрисдикції у випадках, коли правопорушення вчинене:

- на її території; або
- на борту судна, яке ходить під її прапором; або
- на борту літака, зареєстрованого відповідно до її законодавства; або
- одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої держави [2].

Крім цього, конвенція не виключає будь-якої кримінальної юрисдикції держав-учасниць відповідно до їх внутрішньодержавного законодавства та не обмежує держави домовлятись про встановлення юрисдикції, ґрунтуючись на будь-яких інших прив'язках.

Схожий, але більш звужений підхід запропоновано у концепції Конвенції про забезпечення міжнародної інформаційної безпеки, що була представлена в Лондоні у 2011 році на конференції з питань кіберпростору. Концепція визначила лише три наступні прив'язки:

- якщо протиправне діяння здійснено на території відповідної держави;
- на борту судна, що ходить під прапором цієї держави;
- на борту літака чи іншого літаючого апарату, зареєстрованого відповідно до законів тієї держави [3].

Як і в Конвенції Ради Європи у концепції передбачено проведення консультацій між державами у випадку, якщо на ймовірного правопорушника претендує більш, ніж одна держава-учасник.

Найдетальніший підхід до розмежування юрисдикцій закріплено у проекті Стенфордської міжнародної конвенції щодо посилення захисту від загроз кіберзлочинності та тероризму. Цей проект передбачає, що держави-учасниці повинні вживати всі необхідні заходи для встановлення юрисдикції щодо злочинів, передбачених відповідними статтями проекту конвенції в наступних випадках:

- злочин скоєно на території цієї держави або на борту судна, літака чи супутника, зареєстрованого в цій державі або в будь-якому іншому місці, якщо її юрисдикція визнається нормами міжнародного права;
- ймовірний злочинець є громадянином цієї держави;

- ймовірний злочинець є особою без громадянства з постійним місцем проживання та території цієї держави;
- ймовірний злочинець знаходиться на її території і він не підлягає екстрадиції відповідно до положень цієї конвенції;
- злочин було вчинено з метою нанесення серйозної шкоди цій державі, її громадянам або ж змусити таку державу вчинити чи утриматись від вчинення будь-якої дії;
- злочин має суттєві наслідки для цієї держави.

Крім цього, проект стенфордської конвенції не виключає здійснення будь-якої кримінальної юрисдикції відповідно до національного законодавства або ж двосторонніх чи багатосторонніх міжнародних договорів. Цікавим є те, що у проекті конвенції встановлено наступну послідовність юрисдикцій для держав-учасниць:

1. держава, на території якої фактично перебував злочинець в момент, коли було скоєно ймовірний злочин;
2. держава, якій було заподіяно значну шкоду в результаті ймовірного правопорушення;
3. держава переважного громадянства ймовірного злочинця;
4. держава, на території якої ймовірний злочинець може бути знайденим;
5. будь-яка інша держава-учасниця з ґрунтовними підставами для встановлення її юрисдикції [4].

Зазвичай, коли мова йде про визначення юрисдикції, то науковці посилаються на 2 загальних принципи, а саме: принцип державного суверенітету та територіальної цілісності, відповідно держави мають виключну юрисдикцію в межах своєї території. Звідси також випливає, що законодавча юрисдикція має за основу принцип територіальності та/або національності. Принцип територіальності, в свою чергу, розділяють на суб'єктну (відповідно до суб'єкта вчинення злочину) та об'єктну (відповідно до об'єкта вчинення злочину) територіальність.

Проте, аналізуючи питання розмежування юрисдикцій в інформаційному просторі науковці часто звертаються до принципу універсальної юрисдикції, а також можливість застосування юрисдикції Міжнародного кримінального суду. Принцип універсальної юрисдикції передбачає, що кожна держава може переслідувати правопорушників від імені міжнародної спільноти за вчинення певних видів злочинів, навіть у разі відсутності юрисдикційної прив'язки, або у випадку, коли держава, яка має юрисдикцію не в змозі або не бажає притягнути винних до відповідальності. Таким чином, цей принцип служить додатковим інструментом в колективній системі кримінального правосуддя з метою уникнення безкарності осіб за злочини проти людства. Цей принцип можна було б застосовувати і до кіберпростору у випадку масштабної кібератаки. А у разі наявності у кібератаки ознак акту агресії та/чи порушення норм міжнародного гуманітарного права доцільно було б

поширити юрисдикцію Міжнародного кримінального суду на такі атаки [5; 278].

Неодноразово в науковому співтоваристві висловлювались думки про можливість виокремлення кіберпростору у четвертий міжнародний простір за аналогією із Антарктикою, відкритим морем та космічним простором. Найбільше аналогій проводиться із регулюванням поведінки у відкритому морі.

Певну політичну напругу викликає питання перетину національних юрисдикцій, йдеться про випадки, коли кілька держав бажають поширити свою юрисдикцію та притягнути до відповідальності винних осіб, такі питання, безумовно, повинні вирішуватись на основі домовленостей між зацікавленими сторонами [5; 271].

Підводячи підсумок хотілося б зазначити, що науковцям та міжнародному співтовариству варто було б більше уваги приділяти питанням розмежування систем державного суверенітету та реалій інформаційного простору з точки зору міжнародного права. Кількість загроз міжнародній інформаційній безпеці зростає з кожним днем, а інформаційна злочинність вражає своєю чисельністю та масштабністю. Тому, з метою уникнення негативних наслідків як для окремих держав, так і для міжнародного співтовариства в цілому необхідно звернути увагу на розробку правових механізмів протидії загрозам в інформаційному просторі, зокрема на питання розмежування юрисдикцій в інформаційному просторі.

Література

1. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року [Електронний ресурс]. – // Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=28340.

2. Європейська конвенція про кіберзлочинність від 23 листопада 2001 року [Електронний ресурс]. – // Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575/page.

3. Проект Конвенции об обеспечении международной информационной безопасности (концепция) [Електронний ресурс]. – // Режим доступу: http://www.scrf.gov.ru/documents/6/112.html.

4. Sofaer A. D., Grove G. D., Wilson G. D. Draft International Convention to Enhance Protection from Cyber Crime and Terrorism [Електронний ресурс] / A. D. Sofaer, G. D. Grove, G. D. Wilson. – // Режим доступу: http://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf.

5. Kerschischnig G. Cyberthreats and International Law / G. Kerschischnig // The Hague: Eleven International Publishing. – 2012. – p. 311.

СУЧАСНІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Довгань О.Д.[1], Солодка О.М.[2], Шепета О.В.[3]
[1]НДІІП НАПрНУ
[2]НА СБ України
[3]ННІ ІБ НА СБ України

Сьогодні розвиток технологій негативного впливу на інформаційну інфраструктуру відбувається швидше відповідних засобів протидії. Це пояснюється не лише засекречуванням подібних розробок у найбільш просунутих у комп'ютеризації країнах, використанням їх насамперед в оборонних інтересах. Значною мірою розробка засобів протидії кіберзагрозам у більшості держав із рівнем комп'ютеризації, еквівалентним українському, відбувається пасивно. Це пояснюється, насамперед, недостатнім усвідомленням наявних небезпек на рівні прийняття загальносуспільних рішень, що, у свою чергу, є наслідком недостатньої комп'ютерної грамотності, недостатнього усвідомлення ролі комп'ютеризації у сучасному суспільстві.

При цьому, все ж основними негативними факторами технічного характеру, що впливають на забезпечення захисту національної інформаційної інфраструктури від кіберзагроз в сучасних умовах, є:

- відставання в розробці і впровадженні нової вітчизняної техніки, програмних продуктів, зокрема спрямованих на нейтралізацію наявних кіберзагроз (програм «антивірус» тощо), інформаційних технологій та недостатнє забезпечення у зв'язку з цим ефективного функціонування інформаційної основи розвитку суспільства;
- повільне впровадження новітніх зарубіжних техніко-технологічних здобутків у процес інформатизації в Україні, використання їх без необхідної в інтересах нашого суспільства адаптації, що негативно впливає на вітчизняний інформаційний суверенітет, безпеку національної інформаційної інфраструктури;
- недостатня участь у міжнародному інформаційному співробітництві, зокрема техніко-технологічному, що на сьогодні є важливим стимулом розвитку науково-технічного прогресу. Налагодження рівноправного співробітництва відповідно до національних інтересів України має сприяти піднесенню технологічного рівня вітчизняної інформаційної діяльності до потреб сучасності, до забезпечення ефективного функціонування національної інформаційної сфери.

Ще одна причина осучаснення злочинності пов'язана зі стрімким розвитком інформаційних технологій. Вони сприяли виникненню нового виду злочинності – комп'ютерної, а перехід на методи електронного управління технологічними процесами – появі нового виду тероризму – кібертероризму. Кібертероризм – це різновид тероризму, в основу якого

покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства [1]. На думку С. Хоффмана міжнародний тероризм виявився можливим завдяки широкому набору засобів комунікації [2].

Актуальність проблеми кібертероризму для України подвійна: з одного боку, держава не настільки багата, щоб переобладнати сучасними засобами управління свої хімічні підприємства, атомні електростанції та інші критичні й уразливі структури, що зробило б їх невразливими для нападу кібертерористів. З іншого, – формування нової інформаційної інфраструктури, вітчизняної системи баз суверенної інформації стає стратегічним ресурсом, який вимагає постійної уваги з боку держави.

Варто зазначити, що у швидкоплинному перебігу подій суспільного життя, з революційними процесами у розвитку інформаційних технологій значна частина чинних нормативних актів як внутрішньодержавних, так і міжнародних поступово втрачає актуальність, відповідність процесам, які ними нормуються, і потребує уточнень або ж перегляду. Розвиток інформаційної діяльності створює необхідність правового урегулювання нових аспектів цієї діяльності. Потребує досконалого правового обґрунтування питання організації ефективного протистояння кібертероризму в умовах активізації глобальних впливів, нових інформаційних технологій. Комплекс відповідних правових актів має постійно вдосконалюватися із урахуванням відповідного міжнародного законодавства, його еволюції і вітчизняної законотворчої практики, що має бути на варті інтересів національної інформаційної діяльності.

Оскільки процес протидії сучасним кіберзагрозам – явище багатоаспектне і належить до категорії життєво необхідних, в умовах переходу до інформаційного суспільства, цей процес має спиратися на комплексну систему організаційних заходів. Серед них найбільш актуальним є організація ефективної роботи загальноукраїнського центру аналізу інформаційних, зокрема і кіберзагроз, координації роботи з їх нейтралізації. Такий координаційний центр має організовувати відстежування загроз, вивчення тенденцій їх розвитку, значення їх реального і потенційного впливу на інформаційну структуру, забезпечувати прогноз розвитку ситуації і розробку змісту заходів на попередження. Він повинен мати можливості для ефективного залучення до справи боротьби з кібертероризмом відповідні державні установи, приватні економічні структури, що спеціалізуються на проблемах охоронної діяльності, громадські співтовариства протидії негативним впливам на діяльність інформаційної сфери, надавати суспільно важливу інформацію із цього питання для ЗМІ.

Невпорядкованість процесу доступу до мережі Інтернет державних органів, підприємств, установ та організацій, які отримують, обробляють, поширюють і зберігають інформацію з обмеженим доступом, створює умови

для розміщення державних Інтернет-ресурсів на технічних майданчиках, які не мають відповідного рівня захищеності, особливо це характерно для органів місцевого самоврядування[3].

У зв'язку з цим першочерговим питанням є формування організаційно-правових засад побудови системи захисту критичної інфраструктури від кібернетичних атак**.** Її завданнями мають бути визначення об'єктів вітчизняної інфраструктури, що потребують першочергового захисту від кібернетичних загроз з урахуванням іноземного досвіду, визначення критеріїв їх віднесення, класифікація за категоріями, обґрунтування пропозицій щодо законодавчого регламентування захисту вітчизняної інфраструктури від протиправних кібернетичних посягань.

Сьогодні багато елементів критичної інфраструктури держави знаходяться у сфері володіння приватного сектору і не є державною власністю. Тому вкрай важливим моментом в організації системи забезпечення безпеки держави є створення відповідної системи координації, до складу якої б входили як урядові, так і громадські організації із залученням комерційних структур, які працюють у ключових секторах критичної інфраструктури держави. Тісний взаємозв'язок між державним і приватним сектором країни є невід'ємною умовою безпеки держави[4].

З огляду на те, що кібератаки зазнають постійних змін, їх складно прогнозувати та відстежувати у реальному часі, гостро постає питання вдосконалення системи забезпечення інформаційної безпеки. Досягнення поставленої мети потребує наукового опрацювання та подальшого супроводження таких напрямів, як:

- розвиток захищених телекомунікаційних систем;
- підвищення надійності спеціального програмного забезпечення;
- розробка адекватних методів контролю ефективності засобів захисту інформації;
- виявлення технічних пристроїв і програм, що становлять небезпеку для штатного функціонування інформаційно-телекомунікаційних систем;
- запобігання перехопленню інформації технічними каналами;
- формування системи моніторингу показників якості захисту інформації тощо.

Література

1. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: моногр. / В.О.Голубєв. – Запоріжжя: ГУ "ЗІДМУ", 2003. – 250 с.; Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности [Электронный ресурс] / Е.Старостина. – Режим доступу: http://www.crime–research.ru/articles/starostina**.**

2. Хоффман С. Столкновение глобализаций : Как сделать мир болем пригодным для жизни. Новая парадигма? [Электронный ресурс] / Хоффман С. – Режим доступа: http//www.imperativ.net/imp11/Hoffman.html

3. Петров В. Стан захищеності інформаційних ресурсів України та шляхи її вдосконалення // Актуальні проблеми міжнародної безпеки: український вимір. – К.: ВД «Стилос», 2010. – С. 577.
1. Сайтарли Т. Захист критичної інфраструктури – складова частина національної безпеки і стабільності [Електронний ресурс] / Т.Сайтарли. – Режим доступу: http://www.crime–research.ru/library/Saytarly aprl.htm.

МУЛЬТИАГЕНТНЫЕ МОДЕЛИ ИНФОРМАЦИОННОГО ВЛИЯНИЯ

Додонов В.А., Ландэ Д.В.
Институт проблем регистрации информации НАН Украины

Введение

Разработка и анализ мультиагентных моделей является одной из основных направлений исследования и управления информационными процессами. Данные модели включают исследование взаимодействия информационных агентов друг с другом, а также с внешней средой. Под агентом понимается любая сущность, которая может воспринимать среду обитания агентов (мир агентной системы как модель более высокого уровня – образ, в данном случае, виртуального мира – информационного пространства) и воздействовать на нее. Информационных агентов часто рассматривают как автономные объекты, действующие по определенному сценарию [1,2]. Обычно предполагается, что отдельный информационный агент может иметь лишь частичное представление об общей задаче и способен решить только некоторую подзадачу. Поэтому для решения сколько-нибудь сложной проблемы, как правило, требуется взаимодействие агентов.

В данной работе рассматривается моделирование такого класса сложных систем, как информационные системы, широко представленные, в частности, в виде так называемых социальных сетей. Информационное пространство представляет собой динамическую документальную систему из связанных по смыслу элементов, образующих в динамике своей эволюции информационные потоки [3], [4], [5]. Основным объектом моделирования информационных потоков [6] сегодня являются их тематические срезы, последовательности документов, соответствующих определенной тематике.

Мультиагентные модели

В работе [2] рассматривается модели отдельные документы ТИП ассоциируются с агентами, жизненный цикл агентов – с жизненным циклом документов в информационном пространстве. Соответственно, пространство агентов ассоциировалось с тематическим информационным потоком.

Предполагается, что в течение дискретных моментов времени происходит эволюция популяции агентов. При этом отдельные агенты могут:

– самозарождаться (рождаться по причинам, возникающим вне рассматриваемого мультиагентного пространства);
– порождать новых агентов;
– «умирать» – исчезать из пространства агентов;
– получать ссылки от других агентов.

Каждый агент обладает «потенциалом», зависящим от его возраста (времени жизни на текущий момент), от авторитетности (ссылок, проставленных на него) и плодовитости (количества порожденных непосредственно им агентов).

Управляющие параметры модели следующие:

1) вероятность «самозарождения» P_1;

2) потенциал агента Pot, зависящий от количества ссылок на него (ns), времени его жизни (t), и количества порожденных им агентов (k): $Pot = \frac{ns + k}{t}$;

3) вероятность «рождения» от существующего: $P_2 \cdot Pot$;

4) вероятность «смерти» агента: P_3 / Pot;

5) вероятность ссылки на агента: $P_4 \cdot Pot$.

Варьирование параметрами управления P_1, P_2, P_3 и P_4 позволили смоделировать приведенные на рис. 2 профили поведения ТИП.

На рис. 3 приведена пример возможной динамики мультиагентой системы: процессы рождения новых агентов от существующих обозначены сплошными стрелками, процессы проставления ссылок на агентов представлены пунктирными стрелками, живые агенты – черными кругами, «метрвые» агетнты к моменту t = 5 – незаполненными окружностями.

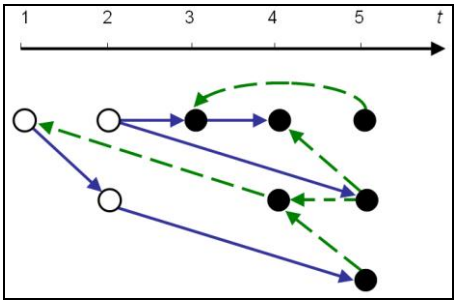


Рис. 1. Фрагмент мультиагентного пространства

Следует отметить, что предлагаемая модель не учитывает:

1) конкуренции агентов внутри агентного пространства (предполагается только сотрудничество путем проставления ссылок и порождения новых агентов);

2) конкуренции разных тематических информационных потоков (учитывается лишь неявно, как причина, обуславливающая параметры функционирования рассматриваемой мультиагентной системы).

Также следует отметить, в предложенной модели учитывается общеизвестная практика проведения информационных кампаний в социальных сетях, заключающаяся в регистрации большого числа аккаунтов-роботов (роя), от имени которых проставляются ссылки (лайки) на материалы, публикуемые от имени аккаунтов из того же роя и на целевые информационные страницы – документы.

В результате проведенных исследований была реализована программа эволюции пространства агентов, исследована эволюция мультиагентной системы при различных значениях параметров, найдены аналогии с реальными тематическими информационными потоками, динамика которых была определена с помощью системы InfoStream.

Модель диффузии информации

Жизненный цикл информационных сюжетов может описываться, например, моделью диффузии информации [6]. Напомним, что в естественных науках под диффузией понимают взаимное проникновение друг в друга соприкасающихся веществ, вызванное, например, тепловым движением их частиц. Процессы диффузии информации, как и процессы диффузии в физике, достаточно точно моделируются с помощью методов клеточных автоматов.

Клеточные автоматы являются полезными дискретными моделями для исследования динамических систем. Дискретность модели, а точнее, возможность представить модель в дискретной форме, может считаться важным преимуществом, поскольку открывает широкие возможности использования компьютерных технологий.

Модель диффузии информации является двумерной, поэтому вся система клеточных автоматов для этого случая будет описываться двумерным массивом. В случае двумерной решетки, элементами которой являются квадраты, ближайшими соседями, входящими в окрестность элемента, можно считать или только элементы, расположенные вверх-вниз и влево-вправо от него, либо добавленные к ним еще и диагональные элементы (окрестность Мура).

В рамках данной модели, которая относится к распространению новостей в информационном пространстве, применяются окрестность Мура и вероятностные правила распространения новостей по заданной тематике. Предполагается, что клетка может быть в одном из трех состояний: 1 – «свежая новость» (клетка окрашивается в черный цвет); 2 – новость, устаревшая, но сохраненная в виде сведений (серая клетка); 3 – клетка не имеет информации, переданной новостным сообщением (клетка белая, информация не дошла или уже забыта).

Модель диффузии информации предполагает следующие правила развития информационного сюжета:

– изначально все поле состоит из белых клеток за исключением одной – черной, которая первой «приняла» новость;

– белая клетка может перекрашиваться только в черный цвет или оставаться белой (она может получать новость или оставаться «в неведении»);

– белая клетка перекрашивается, если выполняется условие: $C \cdot pm > 1$, где p – псевдослучайная величина $(0 < p < 1)$, m – количество черных клеток в окрестности, C – константа ($C = 1{,}5$ при $m = 1$; $C = 1$ при $m \neq 1$);

– если клетка черная, а вокруг нее исключительно черные и серые, то она перекрашивается в серый цвет (новость устаревает, но сохраняется как сведения);

– если клетка серая, а вокруг нее исключительно серые и черные, то она перекрашивается в белый цвет (происходит забывание сведений при их общеизвестности).

На поле размером 40 х 40 (рис. 2, размеры были выбраны исключительно для наглядности) состояние системы клеточных автоматов полностью стабилизируется за ограниченное количество тактов, т.е. на практике процесс оказался сходящимся.

Типичные зависимости количества клеток (последовательности количества однотипных клеток), пребывающих в различных состояниях, в зависимости от шагов итерации приведены на рис. 3.

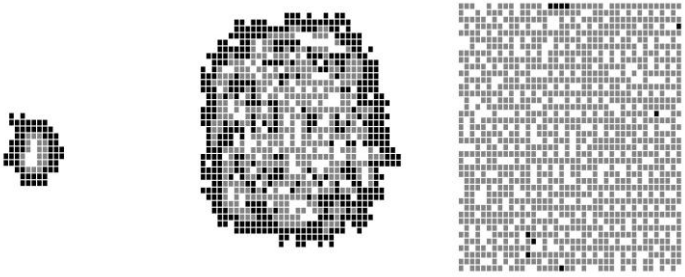


Рис. 2 – Состояния эволюции системы клеточных автоматов

При анализе приведенных графиков следует обратить внимание на такие особенности: 1 – суммарное количество клеток, пребывающих во всех трех состояниях на каждом шагу итерации постоянно и равно размеру поля; 2 – при стабилизации клеточных автоматов соотношение количества серых, белых и черных клеток приблизительно составляет: 0.75 : 0.25 : 0. Именно черные клетки образуют актуальный информационный сюжет, динамика которого представлена на рис. 3.

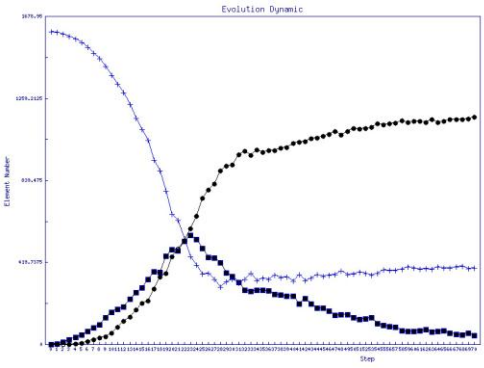


Рис. 3 – Распределение клеток в зависимости от такта системы клеточных автоматов: белые клетки – (+); серые клетки – (●); черные клетки – (■)

Модель динамики информационных операций

Предполагается, что именно нарушение типовой динамики информационных потоков в открытом информационном пространстве может свидетельствовать об информационных воздействиях, информационных операциях [7, 8]. При исследовании информационных операций также большое внимание уделяется анализу динамики тематических публикаций, если есть возможность, с учетом тональности этих публикаций, пользоваться доступными аналитическими средствами, например, вейвлет-анализом. При этом следует ориентироваться на возможные модели информационных атак, например, если эта модель охватывает фазы: «фоновые публикации» — «затишье» — «артподготовка» — «затишье» — «атака» (рис. 4), то уже по первым трем компонентам можно с большой вероятностью предсказать грядущие события.

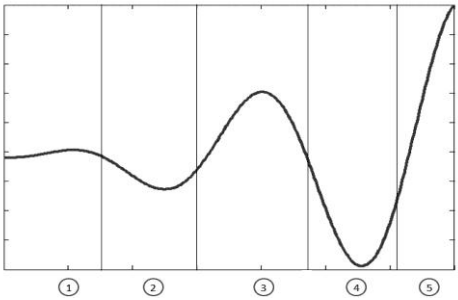


Рис. 4 – Динамика количества тематических сообщений во время проведения информационной операции: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста

Приведенный выше план, очевидно, является идеальным, ориентированным исключительно на данные контент-мониторинга веб-ресурсов.

Конечно, в лучшем положении находятся пользователи профессиональных систем контент-мониторинга. Многие современные информационно-аналитические системы содержат в своем составе средства отображения статистики вхождения в базы данных понятий, соответствующих пользовательским запросам. В частности, авторами использовалась подсистема статистики в рамках системы контент-мониторинга веб-пространства InfoStream, реализующая данную функциональность.

При изучении трендов информационных операций в качестве временных рядов рассматриваются именно ряды по количеству тематических публикаций за определенный промежуток времени, соответствующие этим информационным операциям. Поэтому для выявления трендов исследуются информационные потоки, соответствующие тематикам информационных операций – тематические информационные потоки.

Приведенные в [7] тренды сообщений, соответствующие этапам информационной операции, представлены на рис. 6. При этом аналитики уже по первым трем компонентам (фон» – «затишье» – «артподготовка») могут с большой вероятностью предсказать будущие события.

Следует отметить, что подобная динамика количества тематических сообщений при проведении информационных операций хорошо описывается известным уравнением распространения электромагнитных волн $y = A + Bx\sin(x)$, где x – время, A и B – константы, определяемые эмпирически.

Как известно, в настоящее время инновационная деятельность также косвенно измеряется количеством публикаций, относящимся к инновациям, существует несколько моделей инновационных процессов, среди которых можно выделить модель диффузии инноваций [9]. Вместе с тем, внедрение инноваций также можно считать информационными операциями. Поэтому обратимся к результатам соответствующих исследований. На рис. 5 приведена обоснованная в [10] диаграмма количества публикаций, соответствующая тренду инновационной деятельности.

Объединяя графики, соответствующие началу информационной операции и тренду инновационной деятельности, можно получить полный график, соответствующий отображению информационных операций в информационном пространстве (рис. 6).

Предложенные модели полностью соответствуют реальным данным, которые экстрагируются системами контент-мониторинга. Поэтому приведенные зависимости могут быть использованы в качестве шаблонов для выявления информационных операций – как путем анализа ретроспективного фонда сетевых публикаций, так и путем оперативного мониторинга появления некоторых их признаков в реальном времени.

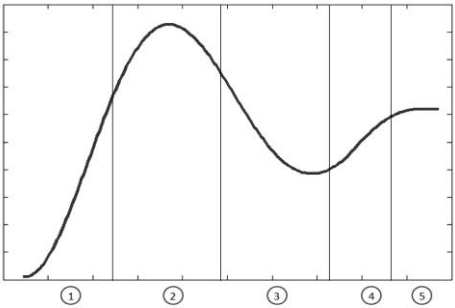


Рис. 5 – Диаграмма количества публикаций, соответствующих тренду инновационной деятельности: 1 – атака/триггер роста; 2 – пик завышенных ожиданий; 3 – утрата иллюзий; 4 – общественное осознание; 5 – продуктивность/фон

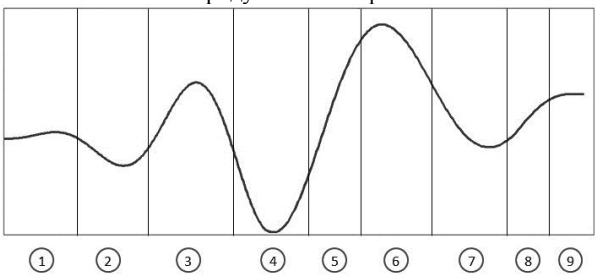


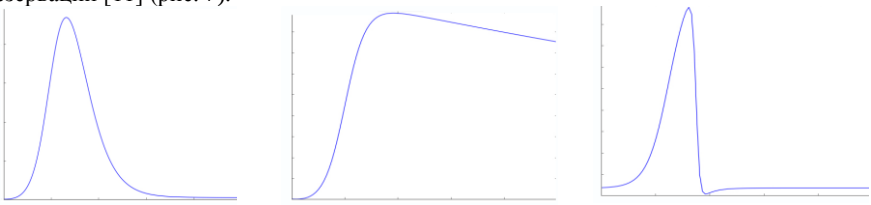
Рис. 6 – Обобщенная диаграмма, соответствующая всем этапам жизненного цикла информационных операций: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста; 6 – пик завышенных ожиданий; 7 – утрата иллюзий; 8 – общественное осознание; 9 – продуктивность/фон

Отметим, что предложенная модель позволяет отличать информационные потоки, поведение которых определяется естественными закономерностями медийного пространства, от потоков, освещение которых в медийных средствах испытывает влияние внешних факторов. В частности, таким индикатором может быть отклонение от характерных форм распределения, появление периодических зон нестабильности значений, соответствующих динамике ТИП, или, наоборот, удивительная локальная стабильность этих значений.

Модель информационных резерваций

Некоторое простое обобщение модели диффузии информации, связанное с восприятием информации, которое приводит к искажению типовой

динамики, что можно объяснять наличием эффекта информационной резервации [11] (рис. 7).



а *б* *в*

Рис. 5 – Динамика количества клеток в состоянии «свежая новость»:
1 – типовая динамика;
2 – растягивание периода актуальности информации;
3 – немедленное прекращение распространения информации.

Таким образом, информационную резервацию можно также характеризовать как область информационного пространства, находящуюся под непрерывным воздействием информационной операции, где динамике информационных потоков по многим важным темам, протекающим в ней, могут быть присущи отклонения от характера плавного «всплеска», а именно:

– быстрое прекращение «нежелательного» информационного потока;

– растягивание периода подъема информационного сюжета «угодной» администрации информационной резервации тематики.

Отсюда следует, что под информационной резервацией можно понимать изолированную часть информационного пространства, плохо связанную с глобальным (общим) информационным пространством, в которой блокируются внешние по отношению к ней информационные потоки и циркулирует собственная информация, не соответствующая той, которая циркулирует во внешней среде (в глобальном информационном пространстве).

Выводы

Построение и анализ мультиагентных моделей взаимодействия информационных элементов представляет исключительный интерес как с точки зрения мониторинга, принятия решения, организации управления информационными атаками и ресурсами, так и в возможности своевременного выявления и прогнозирования результатов информационного воздействия, атак на социальную среду.

Исследования в области мультагентных систем представляют как научный, так и прикладной, насущный интерес. Сложные проблему, возникшую в информационном пространстве, можно понять, только разложив ее на простые факторы, агенты, действующие по определенным правилам, взаимодействие которых и породило проблему. Выявив факторы,

можно встроить их в многоагентные компьютерные модели информационного пространства и экспериментировать с ними, выявлять закономерности, переносимые в мир информационных взаимодействий.

Литература

1. Rahwan T., Michalak T.P., Wooldridge M., Jennings M. R. Coalition structure generation: A survey // Artificial Intelligence, 2015. – Vol. 229. – pp. 139-174.

2. Додонов А.Г., Ландэ Д.В. Мультиагентная модель поведения тематических информационных потоков // Материалы VI Всероссийской мультиконференции по проблемам управления (30 сентября - 5 октября 2013 г.) - Том. 4. - Ростов-на-Дону: Издательство Южного федерального университета, 2013. - С. 102-107.

3. Del Corso G.M., Gulli A., Romani F. Ranking a Stream of News. In Processing of the 14th International World Wide Web Conference, 2005.

4. Kleinberg J. Temporal dynamics of on-line information streams // Data Stream Management: Processing High-Speed Data Streams. – Springer, 2006.

5. Lande D., Braichevski S, Busch D. Informationsfluesse im Internet // IWP - Information Wissenschaft & Praxis, 59(2007), Heft 5. – S. 277-284.

6. Ландэ Д.В., Снарский А.А., Брайчевский С.М., Дармохвал А.Т. Моделирование динамики новостных текстовых потоков // Интернет-математика 2007: Сборник работ участников конкурса. – Екатеринбург: Изд-во Урал. ун-та, 2007. – С. 98-107.

7. Горбулін В.П. , Додонов О.Г. , Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. – К.: Інтертехнологія, 2009. – 164 с.

8. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. - К.: ИПРИ НАН Украины, 2013. - 248 с.

9. Bhargava S.C., Kumar A., Mukherjee A. A stochastic cellular automata model of innovation diffusion // Technological forecasting and social change, 1993. – 44. – № 1. – P. 87-97.

10. Хорошевский В.Ф. Семантические технологи: ожидания и тренды // Открытые Семантические технологии проектирования интеллектуальных систем – Open Semantic Technologies for Intelligent Systems (OSTIS-2012): материалы II Между-нар. научн.-техн. конф. (Минск, 16-18 февраля 2012 г.). – Минск: БГУИР, 2012. – С. 143-158.

11. Додонов А.Г., Ландэ Д.В. Модель информационной резервации // XV Международная научная конференция имени Т.А. Таран "Интеллектуальный анализ информации" ИАИ-2015, Киев, 20-22 мая 2015 г.: сб. тр. - К. : Просвіта, 2015. - С. 52-57.

КОНТЕНТ-МОНИТОРИНГ КАК ИНСТРУМЕНТ КОНКУРЕНТНОЙ РАЗВЕДКИ НА ПРИМЕРЕ АНАЛИЗА ПРОЦЕССОВ СЛИЯНИЙ И ПОГЛОЩЕНИЙ

Додонов Е.А.
Институт проблем регистрации информации НАН Украины

Конкурентная разведка представляет собой особый вид информационно-аналитической работы, позволяющей собирать разностороннюю информацию без применения специфических методов оперативно-розыскной деятельности, которые являются прерогативой правоохранительных органов [1].

Вместе с тем, применение конкурентной разведки оправдывается не только соображениями безопасности компании, но важно и для решения задач менеджмента и маркетинга тем, что обеспечивает:

– наблюдение за репутацией;

– активное участие в формировании имиджа компании, ее информационного поля;

– отслеживание появления нового конкурента, технологии или канала сбыта;

– выявление возможных слияний и поглощений;

– оценка потенциальных рисков при инвестициях;

– опережение шагов конкурентов в рамках маркетинговых кампаний;

– опережение конкурентов в тендерах;

– выявление каналов утечки информации и др.

Основные задачи систем конкурентной разведки применяются к таким основным объектам:

– партнеры, акционеры, смежники, союзники, контрагенты, клиенты, конкуренты;

– объединения компаний, слияния, кризисные ситуации, поглощения;

– кадровый состав, как своей компании, так и партнеров, конкурентов и т.д., а также кадровые изменения, их динамика;

– торговый оборот, бюджет и его распределения по пунктам;

– заключенные договора, соглашения или договоренности.

В рамках данной работы рассматриваются возможности применения средств контент-мониторинга социальных сетей к процессам слияния и поглощения компаний. Слияния и поглощения (mergers and acquisitions, M&A) – это класс экономических процессов укрупнения бизнеса и капитала, происходящих на макро- и микроэкономическом уровнях, в результате которых на рынке появляются более крупные компании взамен нескольких менее значительных.

Информация о том, какие компании поглощаются, планируют поглотить или ведут переговоры о поглощении можно получить, в частности, или Антимонопольном комитете (АМК) Украины, в антимонопольных службах

других государств, либо по новостным сообщениям, размещаемых в социальных сетях и на соответствующих веб-ресурсах.

С помощью средств контент-мониторинга информация о M&A может быть получена и проанализирована с помощью решения следующих задач:

– Нахождение релевантных публикаций по тематике M&A.

– Определение динамики тематических публикаций.

– Определение критических точек в динамике тематических публикаций.

– Выявление объектов M&A.

– Выявление и визуализация взаимосвязей событий и объектов мониторинга.

– Прогнозирование развития событий на рынке M&A.

Этапы информационно-аналитического исследования

В соответствии с приведенными выше задачами предлагается выделить следующие этапы информационно-аналитического исследования [2]:

1. Выбор системы контент-мониторинга.
2. Формирование запроса в среде выбранной системы. Нахождение тематических публикаций.
3. Определение динамики тематических публикаций по запросу о процессах M&A.
4. Определение критических точек в динамике тематических публикаций.
5. Определение основных событий в критических точках.
6. Выявление объектов M&A.
7. Выявление и визуализация взаимосвязей.
8. Прогноз развития событий.

Рассмотрим эти этапы подробно.

1. В настоящее время самыми эффективными для решения задач анализа динамического контента являются специализированные системы интеграции сетевого контента [3]. В частности, в рамках исследований использовались система контент-мониторинга веб-ресурсов InfoStream (www.infostream.ua) и система мониторинга социальных сетей S-monitor (www.s-monitor.com).

2. Массив тематических документов (тема – M&A в Украине, 2015 г.) выбирается путем ввода запроса на языке данных систем:

((слиян&поглощен)|(злиття&поглинанн))&(Украин|Україн|Киев|Київ)

по которому в период за с января по октябрь 2015 года было опубликовано около 5 тысяч тематических публикаций на веб-сайтах (рис. 1).

Рис. 1 – Фрагмент поискового интерфейса системы InfoStream

Система InfoStream обеспечивает поиск, а также просмотр списка и полных текстов релевантных документов.

3. Режим динамики событий системы интеграции интернет-ресурсов позволяет получить данные о количестве публикаций по заданному запросу за указанный промежуток времени. Эти данные могут быть загружены в настольную систему обработки данных и отображаются в виде графика. В интерфейсе пользователя обеспечивается переход к просмотру релевантных документов по выбранной дате. После этого данные временной динамики за каждые сутки нормируются, т.е. в среде системы Excel формируется временной ряд, содержащий относительные значения, равные отношению количества тематических сообщений к общему потоку сообщений за сутки.

4. Критические точки как локальные максимумы временного ряда динамики публикаций можно определить, например, визуально по графику. Вместе с тем, существуют несколько научно-обоснованных методик, базирующихся на методах цифровой обработки сигналов.

5. Для выявления степени «близости» фрагментов исследуемого временного ряда приведенной диаграмме в различных масштабах предлагается использовать так называемый «вейвлет-анализ» [4], который в настоящее время нашел широкое применение как в естественных науках, так и в социологии [5]. Главная идея вейвлет-преобразования заключается в том, что нестационарный временной ряд разделяется на отдельные промежутки (так называемые «окна наблюдения»), и на каждом из них вычисляется величина, показывающая степень близости закономерностей исследуемых данных с разными сдвигами некоторого вейвлета (специальной функции) в разных масштабах. Вейвлет-преобразование генерирует набор коэффициентов, которые являются функциями двух переменных: времени и частоты, и потому образовывают поверхность в трехмерном пространстве. Чем ближе от анализируемой зависимости в окрестности данной точки к

виду вейвлета, тем большую абсолютную величину имеет соответствующий коэффициент. Применение этих операций, с учетом свойства локальности вейвлета в частотно-временной области, позволяет анализировать данные на разных масштабах и точно определять положение их характерных особенностей во времени. На скейлограмме видные все характерные особенности исходного ряда: масштаб и интенсивность периодических изменений, направление и значение трендов, наличие, расположение и продолжительность локальных особенностей. Следует отметить, что инструменты построения вейвлет-спектограмм доступны как в ряде пакетов математических программ, например, в Matlab, так и через Интернет в режиме онлайн (http://ion.researchsystems.com/cgi-bin/ion-p?page=wavelet.ion).

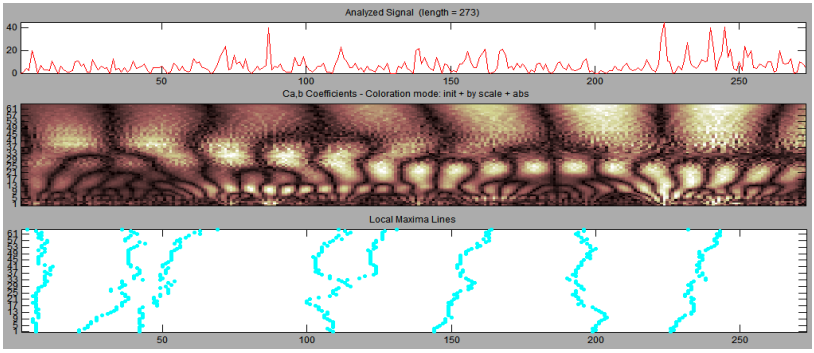


Рис. 2 – Вейвлет-спектограмма исследуемого временного ряда (вейвлет Морле)

6. После определения критических точек с помощью системы контент-мониторинга выполняется построение основных сюжетных цепочек из сообщений, соответствующих запросу за выбранные даты. Таким образом определяются основные события за указанные даты (рис. 3).

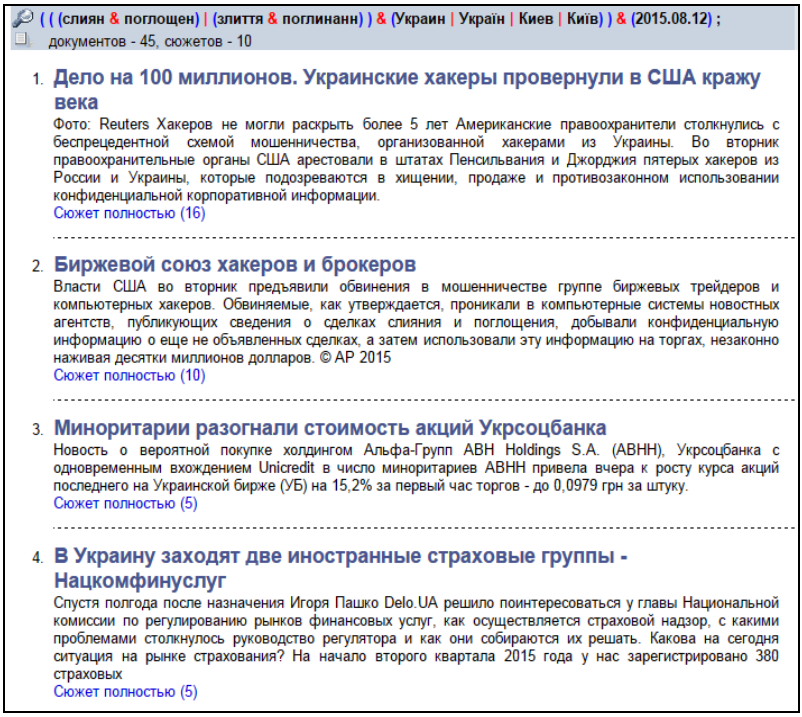


Рис. 3. Фрагмент сюжетных цепочек за 12 августа 2015 г.

7. С помощью методов экстрагирования фактических данных, применяющихся в системах интеграции интернет-ресурсов, в интерфейсе пользователя формируются так называемые «информационные портреты», охватывающие списки персон, топонимов, языков, компаний и т.п., содержащиеся в документах, релевантных некоторому заданному запросу. В нашем случае из «информационного портрета», соответствующего тематическому запросу выбираются наиболее упоминаемые персоны и/или веб-ресурсы за выбранные даты. Эти списки могут агрегироваться, в результате чего возможно определение взаимосвязей событий и объектов.В качестве системы визуализации авторами выбрана система анализа и отображения сетей Gephi (www.gephi.org).

8. Для решения задач прогнозирования перспективным представляется применение теории фракталов при анализе

информационного пространства [6]. Анализ самоподобия информационных массивов может рассматриваться как технология, предназначенная для осуществления аналитических исследований с элементами прогнозирования, пригодная к экстраполяции полученных зависимостей.

Выводы

В докладе представлена методика аналитического исследования процессов M&A, которая базируется на использовании современных инструментальных средствах анализа и визуализации информационных потоков и временных рядов. Как показывает опыт, применение данного подхода при исследовании контента и структуры информационных ресурсов сети Интернет позволяет существенно повысить эффективность аналитической деятельности. Предложенная методика позволяет решить сформулированную задачу, ее можно использовать в качестве основы для проведения аналитической и прогнозной деятельности на основе исследования контента современных компьютерных сетей. В дальнейшем на основе полученных результатов планируется разработка моделирующего комплекса.

Литература

1. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях.– К.: ИПРИ НАН Украины, 2013. – 248 с.
2. Додонов А.Г., Ландэ Д.В., Бойченко А.В. Сценарный подход при исследовании динамики информационных потоков в сети Интернет // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2015): материалы V междунар. науч.-техн. конф. (Минск 19-21 февраля 2015 года) / - Минск: БГУИР, 2015. - С. 225-230.
3. Ланде Д.В. Новітні підходи й технології інформаційно-аналітичної підтримки прийняття рішень // Національна безпека: український вимір: щокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. Безпеки, 2008. – Вип. 1-2 (20-21). – С. 87-105.
4. Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения // Успехи физических наук, 1996. – 166. – № 11. – Р. 1145-1170.
5. Давыдов А.А. Системная социология. – М.: Издательство ЛКИ, 2008. – 192 с.
6. Федер Е. Фракталы. – М., Мир, 1991. – 261 с.

НАЦІОНАЛЬНІ ВИРОБНИКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ФАКТОР ПІДВИЩЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Дубняк М.
НТУУ «КПІ»

Інформаційно-комунікаційни технології все більше проникають у всі сфери людського життя і всі напрямки діяльності сучасної держави. Неможливо уявити подальший розвиток України та її інтеграції у світове співтовариство без розвитку відповідних ІКТ, мереж та структур. Однак, розвиток таких мереж ставить Україну перед новою проблемою – загрози кібернетичного характеру, яким необхідно давати відповідну оцінку, а звідси і вживати адекватних засобів захисту.

Автор вважає, що досягнення кібернетичної безпеки України можливе шляхом створення та запровадження на існуючому комплексі технічних засобів вітчизняного програмного забезпечення або альтернативного програмного забезпечення із відкритим кодом на основі локалізації вже існуючих програм з відкритими ліцензіями. З метою однакового розуміння суті поставленої проблеми слід конкретизувати наступні поняття:

Національне програмне забезпечення — участь у розробці та адаптації операційних систем з відкритим кодом із врахуванням особливостей функціонування вітчизняної ІТ-сфери.

Впровадження власного програмного забезпечення — використання в органах влади всіх рівнів та популяризація серед користувачів (юридичних та фізичних осіб) програмного забезпечення з відкритим кодом.

Законодавчо питання впровадження програмного забезпечення з відкритим кодом врегульовано досить колізійно, та не відповідає критерію єдиного системного підходу, який забезпечить належний рівень захищеності інформаційного простору України від наявних кіберзагроз.

Гарантією національної безпеки є доступ та можливість вітчизняних ІТ-спеціалістів перевірки коду програмного забезпечення, яке буде використовуватись в органах державної влади всіх рівнів. Така перевірка забезпечить контроль над програмним продуктом та забезпечить безпеку інформації, що створюється, використовується, обробляється, передається та зберігається в органах влади, на предмет відсутності спеціальних програмних бек-дорів[1], прихованих шпигунських функцій, направлених на таємний та несанкціонований збір та передачу інформації, що має певний режим доступу та рівень секретності.

Впровадження стратегії переходу на програмне забезпечення з відкритим кодом, та подальший курс на розбудову інформаційної сфери на засадах вільного та відкритого ПЗ, покликаний забезпечити:

економію бюджетних коштів — за рахунок скорочення витрат на закупівлю власницького ПО;

створення робочих місць — необхідна команда IT-спеціалістів, яка здатна забезпечити адаптацію та супровід програмного забезпечення, які не будуть залежати від монополістичних умов постачальників ПО;

дотримання прав інтелектуальної власності — оскільки поширення програмного забезпечення з відкритим кодом висуває до користувачів мінімум ліцензійних умов;

гарантований доступ та захищеність інформації — за рахунок наслідування та незмінності вільних форматів створення та збереження інформації;

можливість використання світового досвіду — спираючись на світову базу програмного забезпечення, що створюється та поширюється (в Інтернеті) на основі вільних публічних ліцензій.

Однак, перехід на програмне забезпечення з відкритим кодом постійно гальмується бюрократичною системою прийняття рішень.

Стаття 20-21 Закону України "Про національну програму інформатизації" визначає особливості закупівлі програмних та технічних засобів для виконання програми інформатизації, а також те, що програмні засоби можуть використовуватись лише в локалізованому вигляді.

Локалізований програмний продукт - приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, стандартами, нормами і правилами, що діють в Україні (стаття 1 вказаного Закону) [1]

Порядок локалізації програмних продуктів затверджений постановою КМУ від 16.11.1998 №1815. більше направлений на вирішення організаційних питань — визначення кола суб'єктів локалізації, механізми фінансування, передачі локалізованого продукту, його тестування та інше.

Однак, Порядок не визначає конкретних вимог щодо приведення у відповідність із законами України та іншими нормативними актами, і загалом зводиться лише до перекладу інтерфейсу програми на державну мову.

На жаль, мова іде одразу про порядок та вимоги щодо закупівлі програмного продукту, і законодавець жодним чином не визначає вимог щодо адаптації чи створення програмного продукту власними силами.

Відсутність державної політики з впровадження програмного забезпечення з відкритим кодом в органи влади всіх рівнів, та тривала співпраця з компанією, що монополізувала ринок програмного забезпечення, призвела до ряду проблем з забезпечення кібербезпеки та інформаційного суверенітету України.

Монополізація ринку, зокрема розпочалась, на думку автора, із підписанням у 2001 році Меморандуму про співпрацю та між Міністерством освіти і науки України та Представництвом Microsoft в країнах СНД.

В рамках першого етапу співпраці (жовтень 2001 - червень 2002) Microsoft створює версії Microsoft Word XP і Microsoft Outlook XP на українській мові та фінансує роботи щодо локалізації програмного забезпечення, а МОН України визначає програмні продукти Microsoft як освітні стандарти в Україні, розробляє навчальні курси з програмного забезпечення Microsoft і впроваджує їх в навчальний процес [2].

2003 року підписується «Меморандум про взаєморозуміння між Міністерством освіти і науки України та Корпорацією Microsoft», за яким поглиблюється комп'ютеризації закладів освіти України шляхом використання в учбовому процесі цих закладів комп'ютерних програм виробництва Microsoft, продукти Microsoft функціонують у системі загальної середньої, професійно-технічної та вищої освіти України, науково-дослідних робіт в галузі інформаційних технологій, в науково-дослідних та вищих навчальних закладах [3].

В листопаді 2013 року було підписано рамкову угоду про співпрацю між Міністерством освіти і науки України та компанією «Майкрософт Україна» на 2013-2018 роки. Документ передбачає проведення низки освітніх ініціатив у закладах дошкільної, середньої та вищої освіти [4]

За відсутності альтернативних навчальних програм щодо вільного та відкритого програмного забезпечення, послідовних та прогностичних рішень щодо інформування населення про такі програми, ми виховали покоління користувачів власницького програмного забезпечення, які не здатні орієнтуватися в середовищі ІТ - загроз, оскільки повністю залежать від продуктів, які нав'язує монополіст. Дійсно, для цілого покоління користувачів компьютеру “Word” став синонімом текстового редактору, без “Outlook Express” вони не уявляють роботу з електронною поштою, а термін “зафотошопити” вживається щодо будь-яких дій з цифровими зображеннями, навіть без належного усвідомлення порядку цін на ліцензію відповідного графічного редактора.

У 2004 році відбулась нарада за участі представників “Майкрософт України”, Держспоживстандарту України, Технічного комітету стандартизації науково-технічної термінології (ТК СНТТ) Держспоживстандарту та Міністерства освіти і науки (МОН) України, інститутів Національної академії наук України (НАНУ), навчальних закладів МОН України, громадських організацій, телерадіокомпанії, преси.

Висновки наради загалом зводяться до поглиблення співпраці в частині “локалізації”-україніації програмних продуктів Майкрософт як от наприклад, перекладу назв програмних продуктів, Вікна чи Віндовз, Служба чи Офіс, Доступ чи Аксес, Провідник чи Експлорер, Майстер чи Візард, Довідка чи Гелп, Слово чи Ворд тощо. Підкреслені назви вже вживають і процес перекладання (транслітерування) назв продовжуватиметься [5].

Однак, важливою рекомендацією наради є звернення до Верховної Ради України та відповідних комітетів про забезпечення законодавчими та нормативними актами сфери розвитку інформаційних технологій і ринку

програмних комп'ютерних продуктів для захисту національних та культурно-освітніх інтересів України.

Завдання для МОН України - запровадити альтернативну програму підтримування розвитку вільного відкритого та безоплатного програмного забезпечення (зокрема зі світовими лідерами у розробці програмного забезпечення IBM, Red Hat, Intel, Novel), щоб уникнути монополізації ринку та загрози національній безпеці [5].

Отже, ще у 2004 році після виконання ряду етапів за першим Меморандумом, стало очевидним і зрозумілим, що тотальна "Майкрософтизація" інформаційної інфраструктури України, яка на той момент робила вже не перші кроки щодо інформатизації, призводить до монополізації ринку, несе загрози національній безпеці та інформаційному суверенітету держави.

Співпраця з компанією Майкрософт дала поштовх до реалізації програми інформатизації, можливо була доцільною на перших етапах. Позитивними рисами співпраці можна назвати такі – забезпечення ліцензійними програмним продуктом, допомога у боротьбі з не легалізованим програмним забезпеченням, безкоштовна локалізація, створення пільгових умов для придбання ліцензій органами державної влади. Однак, негативними рисами такої співпраці є звуженість ринку та відсутність альтернатив, а також постійні витрати з бюджету на оновлення ліцензій. Така співпраця лише приклад того як не прогнозованість рішень дарує ринок монополісту, яким могла б стати і будь-яка інша компанія-виробник пропрієтарного программного забезпечення.

Законодавство України, демонструє рішуче крокування у протилежному напрямку від створення надійної інформаційної безпеки.

Нормативні акти, що визначали основні засади інформаційної безпеки України, або скасовані, або не прийняті взагалі.

Прикладом цього є втрата чинності у 2014 році доктрини інформаційної безпеки України, затвердженої указом Президента від 08.07.2009 року, що визначала основні засади інформаційної безпеки України, які могли бути досягнуті завдяки підтримці вітчиняного виробника інформаційної продукції, інформаційно-телекомунікаційного обладнання, засобів захисту інформації та кібербезпеки, національних операторів телекомунікацій та структур забезпечення інформаційної безпеки, зокрема, шляхом створення нормативно-правових передумов для підвищення їх конкурентоспроможності на світовому та національному ринках інформаційних та телекомунікаційних послуг [6].

Постановою Верховної ради України від 03.04.2003 прийнятий за основу проект закону України "Про Концепцію національної інформаційної політики" який був відправлений на доопрацювання [7].

У 2008 році був запропонований проект Закону України "Про концепцію національної інформаційної політики" яким визначалось пріоритетність розвитку та поширення національних інформаційних технологій, ресурсів,

продукції та послуг, а також політика постійного поліпшення кількості та технічної якості каналів передачі інформації, а також всебічне сприяння, державна підтримка та пріоритетність створення і розповсюдження національного інформаційного продукту, в тому числі за межі України [8].

Після майже 10 річного доопрацювання законопроект "Про державну інформаційну політику" схвалюється за основу 11.01.2011 року, зі зміною назви на "Закон України про основні засади державної інформаційної політики" який відхиляється в липні 2011 року, так і не пройшовши другого читання [9].

Звідси маємо висновок, що Україна (як держава) з 2003 року і до тепер, так і не спромоглась затвердити єдиного напрямку розвитку своєї інформаційної сфери, шляхом ухвалення одного із основоположних документів, який визначав би спрямованість головних завдань та засад послідовної розбудови як законодавства в інформаційній сфері так і здійснення конкретних заходів технічного регулювання таких змін.

Як наслідок, з одного боку, маємо велику кількість нормативно-правових актів, що неузгоджені між собою, а з іншого боку, повну неготовність та нездатність України на адекватну реакцію з боку інформаційних загроз.

Увага на спроби нормативного визначення єдиного курсу розбудови інформаційної сфери приділена не дарма. Зазначений законопроект "Про основні засади державної інформаційної політики" та марні спроби його прийняття, а також "Доктрина інформаційної безпеки України", затверджена указом Президента від 08.07.2009 року, що діяла майже 6 років, тезисно визначали актуальність та необхідність створення і підтримки національного інформаційного продукту.

Як висновок, можна констатувати, що в Україні наразі діє монополія одного виробника програмного продукту. Система освіти зорієнтована на використання та вивчення програмного забезпечення монополіста та сприяє подальшому відтоку вітчизняних ІТ-спеціалістів на виконання аутсорсингових замовлень. За умови відсутності власного чи адаптованого програмного забезпечння, нормативного регулювання сфери програм з відкритим кодом, говорити про дієву перспективу та зацікавленість ІТ-спеціалістів на розробку ПО з відкритим кодом та його подальше впровадження для інформаційної безпеки України, очевидно, неможливо.

Література

1. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР // Офіційний вісник України — 1998. — № 10. — С. 5.

2. Меморандум про співпрацю та між Міністерством освіти і науки України та Представництвом Microsoft в країнах СНД // Електронний ресурс [http://zakon4.rada.gov.ua/laws/show/998_170]

3. Меморандум про взаєморозуміння між Міністерством освіти і науки України та Корпорацією Microsoft http:// Електронний ресурс6 zakon2.rada.gov.ua/laws/show/998_160

4. Про підписання рамкової угоди щодо програмного забезпечення ВНЗ між МОН та компанією "Майкрософт Україна" // електронний ресурс: http://www.kmu.gov.ua/control/publish/article?art_id=247923534

5. Українська локалізація програмних виробів корпорації Майкрософт // Електронний ресурс http://tc.terminology.lp.edu.ua/TK_sem_WinUA.htm

6. Про Доктрину інформаційної безпеки України: Указ Президента // Офіційний вісник Президента України від 20.07.2009 р., № 20, стор. 18.

7. Про концепцію національної інформаційної політики : законопроект 2003 року // Електронний ресурс: http://zakon4.rada.gov.ua/laws/show/687-15

8. Про концепцію національної інформаційної політики: законопроект 2008 року // Електроннийй ресурс: http://comin.kmu.gov.ua/ control/uk/publish/printable_article?art_id=66181

9. Про основні засади державної інформаційної політики: законопроект 2011 року // Електронний ресурс: http://search.ligazakon.ua/ l_doc2.nsf/link1/JF5LF00V.html

1 Бек-дор (англ. back door, чорний хід) в комп'ютерній системі (криптосистемі або алгоритмі) — це метод обходу стандартних процедур аутентифікації, несанкціонований віддалений доступ до комп'ютера, отримання доступу до відкритого тексту, і так далі, залишаючись при цьому непоміченим. Електронний ресурс: http://www.wired.com/2013/09/nsa-backdoor/all/

ЗБЕРІГАННЯ ІНФОРМАЦІЇ: МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ

Забара І.М.
Київський національний університет імені Тараса Шевченка

Серед проблематики сучасних міжнародних інформаційних правовідносин, пов'язаних із використанням (застосуванням) інформації у міжнародних відносинах, окреме місце посідає питання міжнародно-правового регулювання зберігання інформації.

Міжнародно-правові, разом із організаційними, фінансовими, технічними і технологічними, входять до комплексу проблемних питань, що забезпечують інформаційну безпеку як окремих держав, так і світового співтовариства.

Міжнародно-правове регулювання зберігання інформації має свої, притаманні особливості, що відрізняють його від здійснюваних суб'єктами міжнародного права інших видів міжнародної інформаційної діяльності. Особливості міжнародно-правове регулювання зберігання інформації, на нашу думку, можуть бути охарактеризовані наступним чином.

Зазначимо, що у питанні міжнародно-правового регулювання зберігання інформації, йдеться про документовану інформацію, первинні і оброблені данні, документовану інформацію інформаційні ресурси, інформаційні продукти, що надаються державами для накопичення, зберігання і подальшого спільного використання учасниками міжнародних угод.

Зберігання інформації переважно здійснюється міжнародними організаціями, що виступають в якості:

(а) депозитаріїв міжнародних угод (ООН), а також

(б) міжнародних баз даних (ЮНЕСКО, МСЕ, ЮНІДО).

В цих випадках мова йде про зберігання на договірній основі переважно документованої інформації.

Зберігання може також здійснюватись:

(в) міжнародними центрами даних, що утворюються міжнародними організаціями на підставі багатосторонніх міжнародних угод.

Використання міжнародних центрів даних відбувається в тих сферах діяльності, які представляють значний інтерес для держав і потребують широкого співробітництва в питанні міждержавного обміну інформацією.

Зміст інформації, що підлягає обміну в міжнародних центрах даних, визначається положеннями міжнародного договору і, як правило, є пов'язаним з її предметною тематикою. Інформація, що підлягає обміну, може бути на будь-яких носіях - друкованих, письмових, аудіовізуальних, електронних тощо.

В якості прикладу, вартими розгляду є положення щодо Міжнародного центру даних, що функціонує в рамках Організації з Договору про всеосяжну заборону ядерних випробувань.

Утворення Міжнародного центру даних (МЦД) передбачено положеннями Договору про всеосяжну заборону ядерних випробувань 1996 р. Для його належного функціонування кожна держава зобов'язується співробітничати в міжнародному обміні сейсмологічними, гідроакустичними, інфразвуковими даними, а також даними про радіонукліди в атмосфері. МЦД, відповідно до умов Договору 1996 р., має отримувати на постійній основі інформацію з Міжнародної системи моніторингу (МСМ), елементи якої розташовані на території держав-учасниць (до складу МСМ входять глобальна мережа первинних і допоміжних станцій сейсмологічного моніторингу, глобальна мережа станцій гідроакустичного моніторингу, глобальна мережа станцій інфразвукового моніторингу, глобальна мережа станцій радіонуклідного моніторингу і сертифікованих лабораторій; передбачається створення систем електромагнітоімпульсного та супутникового моніторингів).

Умови подальшого використання накопиченої у цьому центрі інформації визначаються низкою спеціальних положень щодо рівного, відкритого, зручного та своєчасного доступу тільки держав-учасниць зазначеного Договору.

МЦД, за умовами Договору 1996 р., наділений повноваженнями, які в питанні щодо зберігання, отримання, обміну і надання інформації передбачає: (а) автоматичне і регулярне направлення державі-учаснику інформації з МЦД або відбір інформації на розсуд держави-учасниці і за відповідним запитанням – добір з накопичених даних МСМ на розсуд держави учасниці; (б) надання накопичених даних за спеціальними запитаннями держав-учасниць з архівів МЦД; (в) сприяння окремим державам-учасницям в ідентифікації джерел конкретних явищ і отриманні відповідної інформації.

Кожна держава-учасниця Договору 1996 р. розглядає в якості конфіденційних інформацію і дані, які вона отримує на довірчій основі і встановлює щодо них особливий режим доступу.

(г) Разом із діяльністю міжнародних організацій із зберігання інформації, сталою була і залишається практика, коли і самі держави беруть на себе повноваження депозитарію: зберігання тексту конкретної міжнародної угоди та документів по її ратифікації (документована інформація).

Передача інформації на зберігання суб'єктами міжнародного права відбувається на договірній, добровільній, паритетній, погодженій основі.

Зазвичай, положення міжнародних угод щодо зберігання інформації можуть передбачати мету, об'єкт, правовий режим, порядок і умови зберігання інформації.

Метою зберігання інформації є накопичення (зібраної, обробленої проаналізованої і архівованої інформації) і наступне надання для використання суб'єктами міжнародного права.

Об'єктом зберігання виступають документована інформація, первинні і оброблені данні, інформаційні ресурси та інформаційні продукти.

Правовий режим інформації визначає умови доступу і поширення накопиченої інформації у відношенні до третіх держав і міжнародних організацій, що не є учасниками відповідного міжнародного договору.

Інформація отримана для зберігання може мати різний міжнародно-правовий режим (інформація з відкритим доступом; інформація з обмеженим доступом (конфіденційна інформація; таємна інформація)).

Крім того, кожна держава-учасник визначає обмежений режим доступу до інформації і даних, які вона отримує від міжнародної організації на конфіденційній основі у зв'язку з виконанням угоди. Використання такої інформації і даних відбувається виключно у зв'язку із реалізацією своїх прав та виконанням прийнятих за угодою обов'язків. Прикладом виступають умови по захисту конфіденціальної інформації («Додаток з конфіденційності») Конвенції про заборону розробки, виробництва, накопичення і застосування хімічної зброї та її знищення 1993 р., на підставі якої було утворено Організацію з заборони хімічної зброї (Гаага, Королівство Нідерландів), яка відповідає за зберігання визначеної договором інформації.

Порядок зберігання інформації передбачає послідовність дій суб'єкта міжнародного права (що виступає в якості депозитарію) щодо дотримання відповідних вимог і правил щодо збереження наданої інформації, первинних і оброблених даних, інформаційних ресурсів та інформаційних продуктів.

Умови щодо порядку зберігання інформації використовується в разі необхідності систематичного обміну інформацією між державами-учасницями договору і створеною міжнародною організацією (міжнародним центром даних). Зазвичай інформація, отримана міжнародною організацією, використовується для контролю за діяльністю держав у певних сферах і, у подальшому, надається державам-учасницям.

Умови зберігання інформації передбачають обов'язки суб'єкта міжнародного права (що виступає в якості депозитарію) щодо забезпечення збереження повноти зберігання інформації та належного фізичного стану носіїв інформації.

Враховуючи, що переважна частина міжнародних угод є безстроковими, передбачається, що зберігання інформації відбувається на постійній основі увесь час дії міжнародного договору.

Проблемні питання щодо зберігання інформації, які постають перед наукою міжнародного інформаційного права, на сьогодні є малодослідженими.

Література

1. Василенко В.А. Основы теории международного права / В.А. Василенко – К.: Вища шк. Головное изд-во, 1988. – 288 с.

2. Договор о всеобъемлющем запрещении ядерних испытаний 1996 г. [Електронний ресурс] – Режим доступу: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N96/219/25/PDF/N9621925.pdf?OpenElement.

3. Конвенция о запрещении разработки, производства, накопления и применения химического оружия и его уничтожения 1993 г. / Действующее международное право: в 3-х т. / [сост. Колосов Ю.М., Кривчикова Э.С.]. – М.: Изд-во МНИ МП, 1997. Т. 2. 832 с.

ОЦІНЮВАННЯ СТАНУ МЕРЕЖІ ІНТЕРНЕТ СТОСОВНО ЗАГРОЗ ЗМІНИ ЇЇ ТОПОЛОГІЇ

Зубок В.Ю.
Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ"
ТОВ "Інформаційний центр "Електронні вісті"

У зв’язку з постійним зростанням ролі мережі Інтернет для суспільства, існує актуальна проблема запобігання зниженню швидкості та надійності доставки даних мережею Інтернет, зокрема, підчас нештатних ситуацій, спричинених як антропогенними так і цілком природними факторами, що можуть негатино впливати на зв’язки між Інтернет-вузлами.

Відомо, що архітектура мережі визначає її топологію, склад мережевих пристроїв, правила їхньої взаємоді. В рамках архітектури визначаються способи кодування інформації, її адресації, керування потоками повідомлень, контроля помилок та механізмів протидії аварійним ситуаціям. Логічний та фізичний способи з’єднання комп’ютерів, кабелів та інших компонентів, які в цілому складають мережу, та інші властивлості мереж, які не залежать від її розміру, визначаються її топологією. Топологія не враховує продуктивність вузлів, довжину та пропускну спроможність гілок, хоча ці фактори є важливими при проектуванні мережі. Проте, поняття проектування навряд чи можна застосувати до Інтернету на сучасному кроці.

Понад 30 років тому вузли та зв’язки справді впроваджувались за попереднім проектом. Пропускна здатність гілок, що складали бекбон мережі, зростала планово і одночасно, а вузли мережі було поділено на три рівні – опорна мережа (core), рівень розподілу (distribution), представлений спеціальними вузлами – точками обміну трафіком, та рівень доступу, до якого під’єднувались кінцеві користувачі та невеликі мережі. Але на сучасному етапі відкритість Інтернету в плані підключення нових мереж, а також багаторічна непохитність основних принципів глобальної маршрутизації народили ряд топологічних феноменів, що характеризують Інтернет як складну мережу. Вивченню феномену безмасштабності, самоподібності, малого світу приділяється значна увага.

Отже, топологія мережі Інтернет не є тривіальною, тому не є тривіальною і проблема підвищення швидкості та надійності передачі інформації в глобальній мережі. Головним критерієм обрання маршруту на рівні глобальної маршрутизації є його довжина що визначається як кількість транзитних вузлів до цілі. Географічне положення вузлів чи чи географічна відстань між ним не враховуються. Зв’язки вузла визначають цього положення в мережі відностно інших вузлів.

В інформаційних системах живучість можна визначити як здатність зберігати та відновлювати виконання основних функцій в заданому обсязі протягом заданого часу в разі змін структури системи або алгоритмів та

умов її функціонування внаслідок несприятливих впливів [1]. Для мережі Інтернет на рівні взаємодії автономних систем збереження функцій – це збереження зв‘язності, тобто можливості передачі даних між будь-якими двома вузлами мережі із прийнятною швидкістю. Аналіз топологічних властивостей свідчить, що різні вузли та зв‘язки відіграють не однакову роль в живучісті Інтернету. Спираючись на широко відомі дослідження Барабаші та Альберта, а також на дослідження малих світів в Інтернеті [2], можна стверджувати, що степеневий розподіл зв‘язків між вузлами та високий показник кластеризації мають самоподібний характер та притаманні як великим, так і малим групам вузлів [3],[4]. В цих групах деяка, відносно мала кількість вузлів, має центральне положення, яке визначається значно більшим ступенем вузла, та (або) значно меншим середнім коротшим шляхом до інших вузлів. Такі вузли називають навантаженими, бо через них проходить переважна більшість коротших шляхів в мережі.

Було неодноразово показано, як видалення будь-якого з «центральних» вузлів в певному сегменті Інтернет негативно впливає на довжину транзитів в мережі, про що свідчить значне зниження показника глобальної ефективності [5]. Існує практичний інтерес до оцінки впливу окремих зв’язків на ефективність мережі.

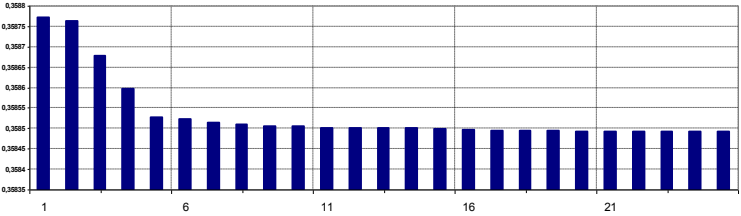
З метою дослідження зв’язку між характеристиками окремих зв’язків Інтернет-вузлами та їх впливом на ефективність мережі було побудовано модель сегменту мережі за даними таблиці маршрутизації мережі обміну трафіком UA-IX. Отримано дані про показники ступеня, середнього шляху та коефіцієнта кластерності вузлів. Були побудовані діаграми, що демонструють динаміку значень ступеню, середнього шляху та коефіцієнта кластерності вузлів, впровадження зв‘язків між якими найбільш вплинуло на глобальну ефективність. Для наочності в діаграмі середнього коротшого шляху (рис. 1,*в*) значення *l* було інвертовано.

Діаграми демонструють відсутність кореляції характеристик вузлів, між якими видалено зв‘язок, та впливом цього видалення на глобальну ефективність. Крім того, впровадження чи видалення *будь-якого невипадкового* окремого зв‘язку для мережі із властивостями безмасштабної взагалі несуттєво впливає на глобальну ефективність.

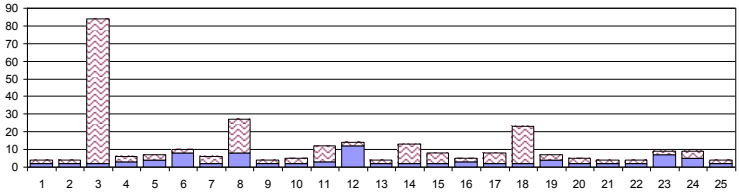
Для підтвердження цього було проведено моделювання видалення зв‘язку між невипадковими вузлами, а саме – обраними за певним критерієм:

1) *за ступенем вузла*. У зв‘язку із степеневим розподілом ступеню, переважна більшість вузлів досліджуваного сегменту має ступінь 1 чи 2. Множину з 545 вузлів ядра мережі було впорядковано за зменшенням ступеню та обрано 10% вузлів з найвищим ступенем, серед яких випадково видалявся один зв‘язок. Експеримент було повторено 100 разів. Результат впливу такого видалення представлено на рис.5. Можна зауважити, що навіть видалення зв‘язку між вузлами-хабами призводить до зниження *E* в межах 0,3%;

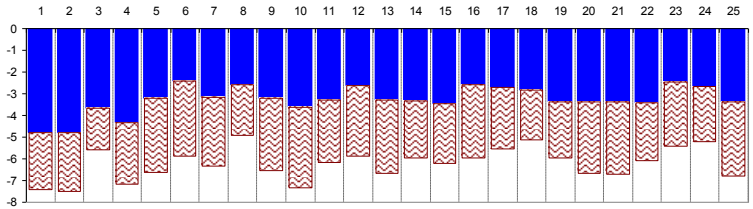
а)



б)



в)



г)

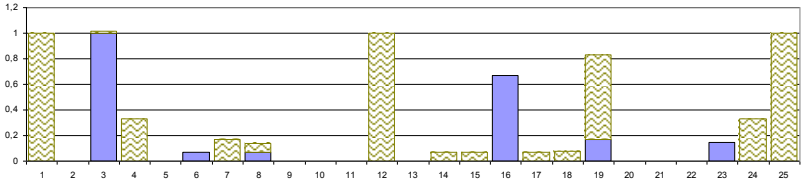
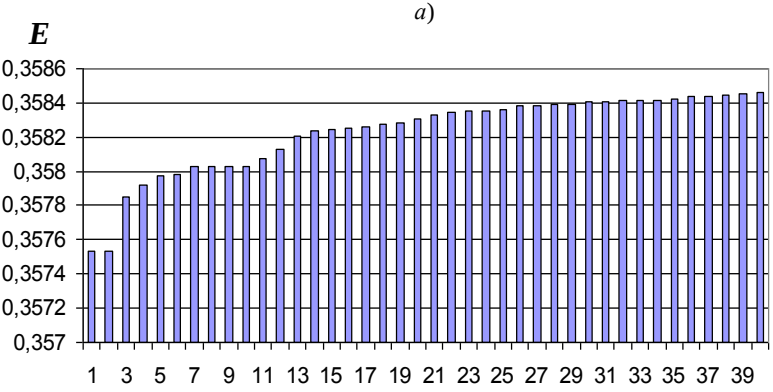


Рис.1. Показник глобальної ефективності *E* при впровадженні зв‘язку між вузлами *i* та *j* (*а*), а також ступені (*б*), середній коротший шлях (*в*), коефіцієнти кластерності (*г*) відповідних вузлів *i* та *j*

2) *за середнім коротшим шляхом*. Множину з 54 вузлів ядра мережі було впорядковано за зростанням показника l_m та обрано 10% вузлів з найменшим l_m, між яких випадково видалявся один зв‘язок. Результат впливу такого видалення представлено на рис.6. Можна зауважити, що навіть в разі видалення зв‘язку між вузлами, що є найважливішими транзитерами, зниження *E* спостерігається в межах 0,5%.

а)



б)

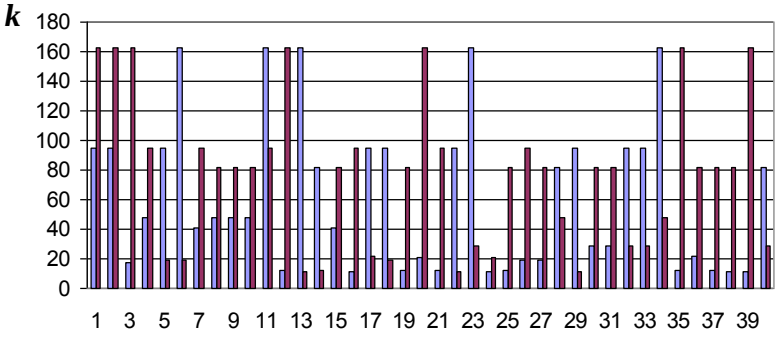
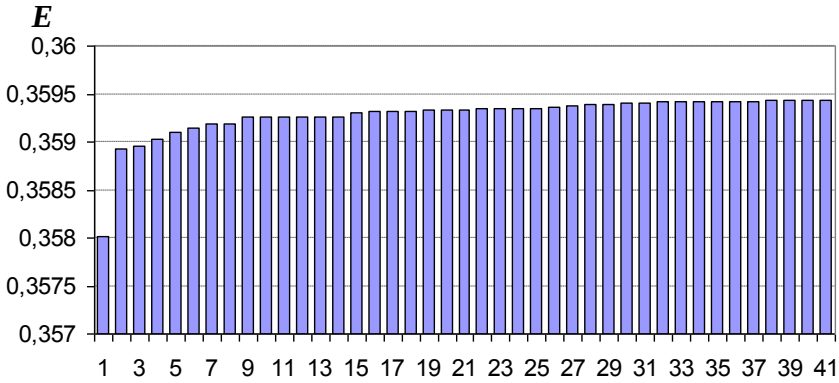


Рис.6. Зміна показника глобальної ефективності *E* при видаленні існуючого з‘єднання між парою вузлів з високими ступенями (*а*) та ступені *k* відповідних вузлів (*б*).

а)



б)

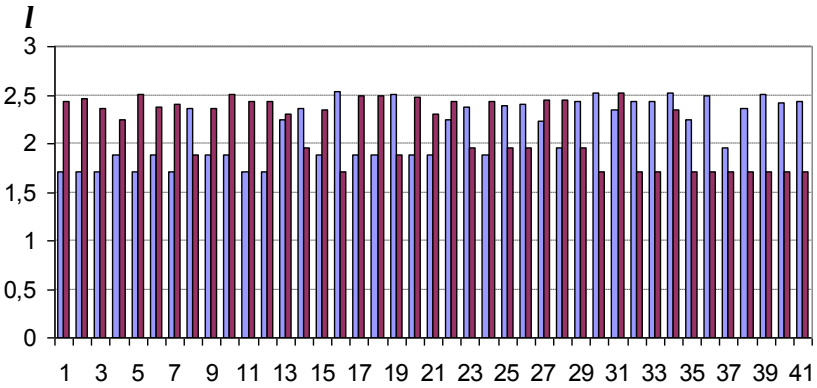


Рис. 6. Зміна показника глобальної ефективності *E* при видаленні існуючого з‘єднання між парою вузлів з найкоротшим середнім шляхом (*а*) та середні шляхи *l* відповідних вузлів (*б*)

Моделювання топологічних змін на моделі сегменту мережі Інтернет демонструє, що, попри високу вразливість до видалення «центральних» вузлів, Інтернет є стійким до навіть спрямованого видалення окремих зв‘язків між будь-якими вузлами, незалежно від навантаження цих зв‘язків.

Література

1. А.Г. Додонов, Д.В. Ландэ. Живучесть информационных систем. — К.: Наук. думка, 2011. — 256 с.

2. Shudong Jin. Small-World Characteristics of Internet Topologies and Implications on Multicast Scaling / Shudong Jin, Azer Bestavros // Computer Networks. – 2006. – Vol.50. – С. 648-666.

3. Зубок В.Ю. Огляд використання математичних параметрів складної мережі для аналізу топології Інтернет / В. Ю. Зубок, О. Т. Дармохвал // Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. – 2010. – №55. – С. 19-28.

4. Зубок В.Ю. Дослідження коефіцієнту кластеризації в глобальній комп'ютерній мережі / В. Ю. Зубок // Збірник наукових праць ІПМЕ ім. Г.Є.Пухова НАН України. – 2012. – №64. – С. 35-41.

5. Зубок В.Ю. Аналіз впливу топології на ефективність та вразливість в глобальних комп'ютерних мережах / В. Ю. Зубок // Інформаційні технології. Безпека. – 2012. – № 2 (2). – С. 17-25.

ЕКСТРЕМІСТСЬКА ДІЯЛЬНІСТЬ У МЕРЕЖІ ІНТЕРНЕТ: ПРАВОВІ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ В УКРАЇНІ

Ірха Ю.Б.
Конституційний Суд України

Стрімкий розвиток інформаційних технологій наприкінці XX–початку XXI століття суттєво вплинув на життя людини, суспільства і держави. Нові способи обміну даними підвищили ступінь та якість поінформованості різних суб'єктів права, розширили можливості для реалізації та захисту прав і свобод, а також контролю за виконанням відповідних обов'язків. Крім того, деякі правовідносини набули нового змісту не тільки на національному, але й на міжнародному рівні.

Інформаційна революція стала одним із ключових факторів утворення глобального інформаційного суспільства, яке фахівцями розглядається, зокрема, як суспільство нового типу, що формується в результаті нової глобальної соціальної революції, основою якої є інтенсивний розвиток і конвергенція інформаційних і телекомунікаційних технологій; суспільство знання, у якому головною умовою благополуччя кожної людини і кожної держави стають знання, отримані завдяки безперешкодному доступу до інформації та вміння з нею працювати [1].

Водночас перехід до нової моделі соціальних відносин супроводжується й негативними процесами. Комп'ютерні технології та Інтернет надали фактично необмежені можливості та ресурси для вільного створення, розповсюдження і зберігання інформації деструктивного характеру. Вони відкрили нові способи маніпулювання інформацією з метою неправомірного впливу на свідомість та поведінку як окремих громадян чи їх груп, так і соціуму. Інтернет став середовищем комунікації екстремістів, терористів, організованої злочинності тощо. Хоча розвинуті держави в Окінавській хартії глобального інформаційного суспільства визнали необхідність спрямування та узгодження зусиль міжнародного співтовариства щодо створення безпечного і вільного від злочинності кіберпростору [2], однак дієвих універсальних чи регіональних правових механізмів для реалізація вказаних задумів досі не створено.

Глобалізаційні перетворення у поєднанні зі світовою фінансово-економічною кризою розкрили значний пласт внутрішніх проблем багатьох держав і, як наслідок, були відновлені або розв'язані економічні, етнічні, культурні, політичні, релігійні та інші конфлікти між представниками різних соціальних груп. У багатьох випадках насильницькі способи й методи вирішення цих конфліктів стали переважати існуючі демократичні стандарти узгодження розбіжностей і протиріч. У державах динамічно почали з'являтися екстремістські угруповання різного спрямування. При цьому саме Інтернет став первинним, а в окремих випадках і пріоритетним

майданом для агітації та пропаганди екстремістських ідеологій; пошуку однодумців, посібників, спільників, спонсорів екстремізму; поширення паніки, страху, чуток у суспільстві; радикалізації населення; руйнування та дискредитації традиційних ціннісних засад, соціальних інститутів, органів публічної влади. Управління Організації Об'єднаних Націй з наркотиків та злочинності наголошує, що екстремістська риторика все частіше переноситься до мережі Інтернет. Відповідний контент поширюється через спеціалізовані веб-сайти, віртуальні чати і форуми, інтернет-журнали, соціальні мережі (Twitter і Facebook), відео і файлообмінники (YouTube і Rapidshare). Екстремістська пропаганда охоплює широкий спектр завдань. Її цільову аудиторію становлять з одного боку потенційні та реальні прихильники екстремістів, а з іншого – їх жертви та супротивники. Окрім пропаганди, Інтернет активно використовується екстремістами для налагодження контактів, організації злочинів. Комунікації відбуваються з використанням спеціального програмного забезпечення, яке запроваджує технологічні бар'єри для входу на відповідні платформи. Захищені паролями веб-сайти значно ускладнюють вчасне виявлення, відстеження та нейтралізацію правоохоронними органам відповідної протиправної діяльності екстремістів [3].

За даними Федерального відомства з охорони конституції Німеччини протягом 2014 року екстремістські організації різного спрямування широко користувалися можливостями Інтернету для пропаганди у державі насильницьких ідеологій та розширення своєї соціальної бази. Ліві та праві екстремісти поширювали у соціальних мережах та інших сегментах Інтернету музику, відео та друковані матеріали для мобілізації своїх прихильників, генерування правильної атмосфери на публічних заходах, ідеологічного обґрунтування своїх вчинків. Такі дії розглядаються як важливий фактор у процесі радикалізації і вербуванні громадян, збільшенні потенціалу екстремістів. Сучасні комунікативні технології використовуються також терористами, як угрупованнями, так і одинаками, для публічного демонстрування своїх «досягнень». До того ж це робиться на досить хорошому професійному рівні [4]. У сучасних умовах активна інформаційна діяльність екстремістських угруповань, у тому числі міжнародних, або екстремістів-одинаків у мережі Інтернет значно загрожує інформаційно-психологічній безпеці індивідів, під якою Я. Жарков розуміє стан захищеності психіки людини від негативного впливу, що здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, та приводить до неадекватного сприйняття нею дійсності [5]. Оскільки гарантування і захист інформаційної безпеки особи і суспільства є складовими національної безпеки, то, очевидно, що держава не може залишити поза увагою питання щодо протидії інформаційним загрозам з боку екстремістів та інших суб'єктів інформаційних відносин.

В Україні інформаційна діяльність в Інтернеті не отримала належного нормативно-правового регулювання. Навіть після анексії Автономної

Республіки Крим та міста Севастополя, тимчасової окупації окремих районів Донецької та Луганської областей у законодавстві не розроблено ефективних механізмів нагляду за цією сферою, своєчасного виявлення і нейтралізації реальних та потенційних загроз національним інтересам. Певні екстремістські угруповання скористалися ситуацією і збільшили свою присутність в інформаційному полі держави, особливо українському сегменті Інтернет, намагаючись посилити свої позицій, здобути певні економічні чи політичні дивіденди, вплинути на внутрішню та зовнішню політику.

У Воєнній доктрині України визначено, що воєнно-політичними викликами, які можуть перерости в загрозу застосування воєнної сили проти України є, зокрема, цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин [6].

Такий вплив здійснюється не тільки ззовні іноземними державами, їхніми збройними силами або спеціальними службами, але й зсередини через контрольовані ними екстремістські та терористичні угруповання, що безпосередньо загрожує незалежності та суверенітету нашої держави.

Враховуючи наведене, вважаю, що для ефективного забезпечення національної безпеки України, відновлення її територіальної цілісності необхідно якнайшвидше : 1) прийняти закон про кібербезпеку; 2) ухвалити нову доктрину з інформаційної безпеки. Ці акти стануть основою для створення системи протидії екстремістській діяльності в Інтернеті.

Література

1. Проскуріна О.О. Глобальне інформаційне суспільство: ідеї та реалії / О.О. Проскуріна // Вісник СевНТУ : зб. наук. пр. Вип. 136/2012. Серія : Політологія. – Севастополь, 2012. – С. 73.

2. Окинавская хартия глобального информационного общества : Хартия, принятая 22 июля 2000 г., г. Окинава [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/998_163.

3. The use of the Internet for terrorist purposes // United Nations Office on Drugs and Crime. – New York, 2012. – [Електронний ресурс]. – Режим доступу: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

4. 2014 Annual Report on the Protection of the Constitution Facts and Trends // Federal Ministry of the Interior. – [Електронний ресурс]. – Режим доступу: http://www.verfassungsschutz.de/embed/annual-report-2014-summary.pdf.

5. Жарков Я. Небезпеки особистості в інформаційному просторі / Я. Жарков [Електронний ресурс]. – Режим доступу: http://webcache.ghttp://www.justinian.com.ua/article.php?id=2554.

6. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 24 вересня 2015 р. № 555/2015 [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/5552015-19443.

ПРОБЛЕМНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

Корж І.
Науково-дослідний інститут інформатики і права НАПрН України

Аналіз мас-медіа та наукових розвідок минулого століття свідчить, що XXI століття очікувалося стати періодом стрімкого зростання значущості науки й освіти в житті людства, кожного суспільства й особистості. Головними тенденціями минулого століття був технічний прогрес, екстенсивне використання природних ресурсів, розширене відтворення та примноження матеріального багатства. Наука базувалася на аналізі, спеціалізації, народження нових наукових дисциплін на стику різних галузей знань.

Водночас суперечливими результатами минулого століття виявилися: величезні науково-технічні досягнення; майже повсюдне підвищення якості життя; утвердження в суспільному житті ліберальних цінностей, прав і свобод людини; небачене зростання напрацьованих і накопичених людством матеріальних цінностей; стрімке зростання населення; існуючі важковирішувані глобальні проблеми.

Очікувалося, що у XXI столітті попередню індустріальну картину світу мали б змінити тенденції до багатополярності світу і глобалізації економіки та фінансів, до стрімкого розвитку у сфері науки і техніки, різні інновації, а також поява економічних знань. Саме підвищення якості і масштабів економіки і науки мали б стимулювати прогрес у науці і техніці. Ярко вираженими тенденціями мали б стати інтернаціоналізація господарського життя, транснаціоналізація бізнесу, інтеграція національних господарств. На заміну існуючим мають прийти безвідходні, малоенерго- і матеріаломісткі екологічно чисті технології, а провідну роль у суспільстві стануть відігравати сфера послуг, наука і освіта. Величезне місце в житті мало отримати виробництво, розподіл і споживання інформації; прогнозувалося поглиблення галузевого і професійного поділу праці; збільшення числа працівників інтелектуальної праці і сервісу. Таким чином, пріоритетами життєдіяльності і розвитку особистості, суспільства, держав, світового співтовариства в XXI столітті мали б стати висока моральність, помірність, обачність, передбачуваність, економія, стійкість, порядок, безпека, недопущення зниження якості життя, особливо в країнах, що розвиваються, здійснення глобального переходу до сталого розвитку, із забезпеченням високої якості життя.

Водночас, поряд із зазначеними оптимістичними очікуваннями, аналіз тенденцій у сфері безпеки людства і людини і прогноз на XXI століття показували, що небезпеки і загрози набувають усе більш комплексного взаємопов'язаного характеру. Тому вбачалося, що в XXI столітті єдино вірним

підходом до вирішення проблем безпеки має бути комплексний, системний підхід.

Говорячи про комплексне забезпечення безпеки суспільства, людини і навколишнього середовища, мається на увазі забезпечення безпеки від усіх видів небезпек і загроз в рамках єдиної стратегії з використанням повного набору форм і методів протидії їм. Тобто, в цьому розумілося інтегроване її поняття, на відміну від стандартного підходу щодо відповідних сфер: військової, економічної, інформаційної, екологічної тощо. Зазначене передбачає консолідацію зусиль і засобів багатьох суб'єктів міжнародних відносин.

Було очевидне очікування, що:

– зазначені мотиви, цілі і пріоритети розвитку збережуться і в XXI столітті, водночас значення безпеки, її вага в загальній характеристиці якості життя суттєво зростуть;

– забезпечення комплексної безпеки людини, суспільства, держави та світового співтовариства стане найважливішим пріоритетом найближчих десятиліть в XXI столітті, перетвориться в основу стратегії існування цивілізації в сучасних і прогнозованих майбутніх умовах.

Однак світова динаміка явила новий цивілізований феномен. Зростаюча взаємозалежність країн і народів, незважаючи на всі відмінності в рівнях розвитку, культурі, релігії, історичних традиціях досягла такого ступеня, що її стали розуміти як найважливіше сучасне явище в житті людства, назване «глобалізацією». Поряд з позитивними вона має і негативний характер, що проявилося у вигляді так званих глобальних проблем. Завдання, що стояли перед людством у минулому столітті і до цього часу є невирішеними, поглиблюють глобальні проблеми, які несуть істотні загрози безпеці цивілізації, формують у своїй сукупності ту загальносистемну кризу, перед якою нині постали держави і світове співтовариство на початку XXI століття.

Основна частина глобальних проблем в даний час ефективних рішень не знаходить. Вони часом досягають критичного стану і вибухають різного роду лихами. У результаті складаються надзвичайні ситуації різного характеру і масштабу, відбувається дестабілізація умов існування цивілізації, порушуються процеси її розвитку, суспільству завдається великої шкоди, який виражається в людських втратах і економічних збитках. І останні події у світі, насамперед навколо України та Сирії, в країнах Європейського Союзу – є підтвердженням тому.

На початку XXI століття у світі відбуваються кардинальні трансформації, що супроводжуються зміною геополітичних конфігурацій. Глобальна фінансово-економічна криза стала черговим викликом світовій цивілізації, обумовила невизначеність перспектив глобальної та національних економік, прискорила пошук шляхів модернізації суспільних систем. Криза виявила глибинні вади глобальної економічної моделі, сприяла усвідомленню необхідності системних змін світового економічного і соціального порядку. На тлі посилення воєнних загроз і зростання нестабільності у світі постають

нові виклики міжнародній безпеці – у сировинній, енергетичній, фінансовій, інформаційній, екологічній, продовольчій сферах. Такі загрози як поширення зброї масового ураження, міжнародний тероризм, транснаціональна організована злочинність, кіберзлочинність, інформаційні війни, нелегальна міграція, піратство, ескалація міждержавних і громадянських конфліктів стають дедалі інтенсивнішими, охоплюють нові регіони і країни. Зростають регіональні загрози міжнародній безпеці, які за своїми негативними наслідками можуть мати потенціал глобального впливу. Постала небезпечна тенденція перегляду національних кордонів поза нормами міжнародного права що, у свою чергу, зруйнувало напрацьовану до цього міжнародну правову систему взаємовідносин та забезпечення безпеки країн. Використання сили і погрози силою повернулися до практики міжнародних відносин, у тому числі в Європі. Різновекторні геополітичні впливи на Україну в умовах неефективності гарантій її безпеки, наявності біля кордонів «заморожених» конфліктів, а також критичної зовнішньої залежності національної економіки обумовлюють уразливість України, послаблюють її роль на міжнародній арені та виштовхують на периферію світової політики, у «сіру зону безпеки».

Однак сьогодні не менш нагальними і актуальними від зовнішніх залишаються внутрішні виклики національній безпеці. Нерішучі зміни неефективної пострадянської суспільної системи, насамперед державної влади та місцевого самоврядування, викривлення демократичних процедур, що штучно стримувало процеси кадрового оновлення державних органів, масштабна корупція в державних органах обумовили слабкість, а подекуди і неспроможність держави виконувати її функції, насамперед у сфері захисту прав і свобод людини і громадянина, зростаючу недовіру до неї з боку суспільства. З огляду на зазначене, існує нагальна потреба в мінімізації негативного впливу на суспільне життя держави з боку наступних факторів.

Фактори політичного та економічного характеру

Залишається невирішеним одне із актуальних завдань, яке постало в перші роки незалежності України – це відділення бізнесу від політичної влади. Зрощення бізнесу та політичної влади, що виникло в період президентства Л. Д. Кучми, породило елітну економіку (тобто сфери господарювання для обмеженого кола осіб, з високими вхідними бар'єрами, що забезпечують отримання надприбутків). При цьому надприбутки стали, у свою чергу, джерелом винагороди влади за «допомогу» у створенні та утриманні неконкурентних переваг. Це руйнує нормальні ринкові механізми формування підприємницького прибутку, а сам прибуток зменшується, частково перетворюючись на складову корупційної ренти. Нині ситуація навіть усугубилась – олігархи через створені ними політичні партії, не тільки знаходяться при владі, але й домінують в політичній сфері. Фактично в Україні побудовано олігархат – Президент і його близьке оточення, Прем'єр-міністр і значна кількість Українського Уряду, значна кількість депутатів Українського парламенту є олігархами чи наближені до них. За словами

євродепутата від Чехії Милослава Рансдорфа, сьогодні в Україні 100 найбагатших олігархів контролює 38% національного майна, і рівень майнової нерівності серед населення зростає і є жахливим. Находження олігархічних груп при владі є реальною загрозою для України. І як показала практика, кадрові питання в державі теж вирішуються не в інтересах суспільства, а в інтересах олігархів.

Боротьба з корупцією на нинішньому, вкрай складному етапі державного розвитку залишає бажати кращого. Події, пов'язані з корупційними скандалами, що виникли у процесі підбору кадрів до структур, що боротимуться з цим ганебним явищем, в яких замішані вищі посадові особи держави – свідчення тому.

Є необхідність у правовому врегулюванні діяльності, а вірніше, експлуатації творців інтелектуальної власності. Очевидно, що є необхідність у формуванні в Україні для учасників ринкових відносин загальних умов «справедливої» вартості прав інтелектуальної власності. Для цього передусім необхідно сформувати конкурентне середовище, позбавлене неринкових методів боротьби. Необхідно створити в економіці України умов, за яких винагорода власників факторів виробництва відповідатиме вартості корисного внеску відповідних факторів виробництва.

Фактори правового характеру

Напрацьована за роки незалежності правова система держави в нині стала переважно правовою системою обслуговування інтересів громадян-товстосумів, чім простих, пересічних громадян, тобто захисником інтересів меншості, ніж інтересів більшості. «Вимучена» правова реформа, з якої можна виділити такі її основні напрями, як конституційний, судовий, адміністративний, кримінальної юстиції, прокуратури, місцевого самоврядування, постійно зіштовхується із завуалірованим супротивом, штрейкбрехерством з боку різних структур державної влади і, насамперед, з боку олігархічних кіл та їхніх представників. Як зазначає М. Ставнічук, державі конче потрібна систематизація реформ: від економіки, фінансів, соціальної політики – до політичної системи внутрішньої та зовнішньої безпеки. Адже єдиним чинником, що за своєю природою здатен слугувати матрицею реформування всієї країни, є конституційно-правова модернізація.

Фактори безпекового і оборонного характеру

Залишаються невирішеними проблеми удосконалення системи оборонного планування та оборонного замовлення, їх реальне і належне фінансування; потребує удосконалення нормативно-правове забезпечення реструктуризації підприємств ОПК України. Особливої уваги заслуговують питання реформування розвідувальної сфери, що потребує нової моделі, як радикального перерозподілу розвідувальної та контррозвідувальної діяльності, так і зміни формату діяльності контррозвідки з одночасним вивільненням її

від правоохоронних повноважень, а також здійснення належного ресурсного забезпечення реформ (фінансове, матеріально-технічне тощо).

Реорганізація сектору безпеки і оборони нині є одним із пріоритетних напрямів євроатлантичного інтеграційного курсу України. Успішне проведення реформ у цій площині дасть змогу прискорити не тільки реформування всіх інших сфер суспільного життя нашої країни, а й підтвердити незмінність курсу нового керівництва України на входження до трансатлантичних структур безпеки, продемонструвати прихильність нашої держави принципам демократії, відкритості й прозорості в її внутрішній та зовнішній політиці.

Фактори гуманітарного характеру

В країні залишаються невирішеними такі проблемні питання, як мовний аспект, релігійний чинник, фактично існуюче полігромадянство – вирішення яких має конструктивно вплинути на створення української нації. В Україні досі не ухвалено закону, який би визначав засади державної етнонаціональної політики, в тому числі формулював мету, принципи та завдання її правового й змістовного наповнення.

Після поглинання в 1686 р. Московською патріархією Київської митрополії релігійно-церковна сфера українського суспільства зазнала значної модифікації – і не в кращий бік. Розпочалося нищення конфесійного плюралізму, віротерпимості й толерантності, притаманних національному православ'ю; також зазнала ліквідації демократична організація, якої дотримувалася Українська православна церква. Остання перетворилася у складі РПЦ на частину державного апарату, ідеологічний підмурок самодержавства, що проглядається і нині, слугує перепоною державо- і націотворенню. Очевидно, що Україні на шляху просування до Європи явно не вистачає Помісної Православної Церкви – могутньої духовно-ідейної опори Українського народу у справі розбудови громадянського суспільства та зміцнення авторитету нашої держави на міжнародній арені. Така церковна структура, дійсно, спроможна і в сучасному світі бути захисником національних інтересів та справжнім виразником патріотичних почуттів своєї нації.

Зазначені чинники разом із незадовільним станом системи забезпечення національної безпеки, поширенням корупції в органах державної влади перешкоджають розв'язанню нагальних проблем суспільного розвитку, сприяють політичній радикалізації, призводять до зростання екстремістських настроїв і рухів, що у стратегічній перспективі може створити реальну загрозу національному суверенітету і територіальній цілісності України.

ДЕРЖАВНА СИСТЕМА ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА В ОСОБЛИВИХ УМОВАХ

Косогов О.М.
Міністерство оборони України

Система органів державної влади та управління, будучи основним фактором, що регулює суспільні відносини в інформаційно-психологічній та кібернетичній сферах, поряд з основним і пріоритетним об'єктом зовнішньої агресії є центральною ланкою забезпечення інформаційної безпеки та основним інструментом відбиття й припинення будь-яких зазіхань іноземних держав на суверенітет, територіальну цілісність і громадянську єдність суспільства, на його життєво важливі інтереси й перспективи розвитку, на психічне здоров'я нації.

Оскільки в інформаційно-психологічному та кібернетичному просторі такі зазіхання можуть приймати форми інформаційної експансії, агресії або інформаційно-психологічної кампанії, на державу в особі її системи органів влади покладається найважливіший обов'язок своєчасного виявлення загроз інформаційної безпеки, мобілізації сил і засобів громадянського суспільства для захисту державних інтересів і протидії агресії в кожній з її форм, а також організації протидії акціям інформаційної агресії (кампанії) на ранніх стадіях виникнення конфлікту.

Основні завдання центральних органів виконавчої влади в галузі інформаційного протиборства:

розробка пропозицій з визначення державної політики України в галузі інформаційного протиборства, прогнозування, виявлення й оцінка джерел та характеру загроз застосування проти України засобів і методів інформаційного протиборства;

збір розвідувальної інформації щодо використаня перспективних інформаційних технологій об'єктів інформаційної сфери конфронтуючої сторони;

захист воєнно-політичного керівництва України, а також індивідуальної, групової й масової свідомості її населення від застосування конфронтуючою стороною інформаційно-психологічних та інформаційно-технічних засобів і методів впливу;

організація протидії антиукраїнській пропаганді, проведеної, у тому числі, інформаційно-психологічними та кібернетичними засобами та методами впливу;

захист інформаційної інфраструктури України від застосування конфронтуючою стороною інформаційно-технічних засобів і методів впливу тощо;

розробка моделі загроз державним інтересам в інформаційно-психологічній та кібернетичній сферах, заснованої на проведенні глибоких і різнобічних наукових досліджень. Створення такої моделі могло б надати

процесу пошуку, визначення й класифікації вже існуючих загроз і їхніх проявів (моніторингу загроз) цілеспрямований характер, а розробка методичних рекомендацій з виявлення загроз і відстеження розвитку загрозливих ситуацій стала б у руках органів виконавчої влади, що займаються забезпеченням інформаційної безпеки, надійним інструментом, який багаторазово підвищує ефективність і продуктивність роботи;

створення й розробка стратегії проведення інформаційних операцій за мирного часу і в особливий період (за різними ступенями ескалації напруженості міжнародних відносин);

розробка нормативно-правової бази проведення спеціальних операцій в інформаційній сфері, застосування інформаційної зброї, а також форм та способів інформаційної боротьби;

створення системи швидкого реагування на раптові (зненацька виявлені) інформаційні атаки, здатної своїми діями скувати дії противника, змусити його відмовитися від всіх або хоча б від частини своїх планів, перехопити ініціативу та створити найбільш сприятливі умови для проведення власної інформаційної операції;

створення системи забезпечення безпеки комп'ютерних систем управління Збройними Силами України.

Державна система інформаційного протиборства - система узгодженої, цілеспрямованої, керованої з єдиного центра діяльності органів державної влади та місцевого самоврядування, що спрямована на захист державних інтересів і забезпечення безпеки особи, суспільства й держави в інформаційній сфері за умов інформаційного протиборства .

Державна система інформаційного протиборства складається з таких основних компонентів.

1. Система протидії інформаційно-психологічної агресії (кампанії) на ранніх стадіях.
2. Система швидкого реагування на раптово виявлені акції (заходи) інформаційної агресії (кампанії).
3. Система сил і засобів інформаційної боротьби.
4. Державна інформаційна політика в умовах інформаційнї боротьби.

ПРОЗОРІСТЬ ВЛАСНОСТІ У СФЕРІ ТЕЛЕРАДІОМОВЛЕННЯ: ПРІОРИТЕТНИЙ НАПРЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Красноступ Г.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Не секрет, що сьогодні більшість громадян України отримують інформацію за допомогою телебачення. Відсутність відомостей про власників відповідних телерадіоорганізацій не дозволяє визначитись з питанням, наскільки тим чи іншим мовникам можна довіряти. Тому, прозорість відносин власності грає важливу роль для плюралізму аудіовізуальних ЗМІ та демократії в цілому.

Частиною п'ятою статті 4 Закону України «Про телебачення і радіомовлення» встановлені основні принципи державної політики у сфері телебачення і радіомовлення. Передбачено, що держава встановлює дієві обмеження щодо монополізації телерадіоорганізацій промислово-фінансовими, політичними та іншими групами чи окремими особами, а також гарантує захист телерадіоорганізацій від фінансового і політичного тиску з боку фінансово-політичних груп та органів державної влади і органів місцевого самоврядування [1].

Підпунктом 12.4 пункту 12 Резолюції Парламентської Асамблеї Ради Європи «Про виконання обов'язків та зобов'язань Україною» від 5 жовтня 2005 р. № 1466 Парламентська Асамблея Ради Європи ще у 2005 році закликала органи влади України гарантувати прозорість власності на засоби масової інформації [2].

У 2013 р. міжнародна громадська організація Access Info Europe провела дослідження правового забезпечення прозорості відносин власності засобів масової інформації у дев'ятнадцяти країнах Європи та Марокко [3], згідно з яким у більш ніж половині досліджених країн, існуючі правила про компанії і володіння засобами масової інформації не дозволяють представникам громадськості дізнатися, хто справжні власники засобів масової інформації. Так, з двадцяти країн, охоплених дослідженням Access Info Europe, лише п'ять вимагають подробиці власності, які повинні надаватися компетентним органом (Хорватія, Ісландія, Італія, Латвія і Норвегія). Тільки в чотирьох країнах, засоби масової інформації керуються конкретними правилами, які вимагають розкриття відповідної інформації безпосередньо населенню (Австрія, Хорватія, Люксембург і Туреччина). З двадцяти країн в дев'яти громадяни не можуть отримати інформацію про власників засобів масової інформації, лише в шести країнах є можливість отримати інформацію про власників аудіовізуальних засобів масової інформації, і тільки в двох країнах можна отримати інформацію про власників друкованих засобів масової інформації та нових медіа.

За результатами вказаного дослідження Access Info Europe було підготовлено «Десять рекомендацій щодо прозорості власності на засоби

масової інформації» [4], які були поліпшені шляхом консультацій з активістами громадянського суспільства, медіа-експертами, і пройшли перевірку під час обговорення з європейськими чиновниками і парламентаріями в Брюсселі, в тому числі – дуже конструктивно – Парламентської Асамблеї Ради Європи.

Так, для того, щоб громадськість дізналась, хто насправді володіє та впливає на засоби масової інформації, правова база в кожній країні повинна забезпечувати:

1) прозорість власності на засоби масової інформації через розкриття національному регуляторному органові та громадськості інформації, яка повинна включати як мінімум: найменування та контактні дані засобу масової інформації; статутні документи (через веб-посилання на завантажені сканування, якщо необхідно); розмір акцій через поріг в 5 %; ім'я та контактні дані безпосередніх власників з більш 5 % акцій; ідентичність тих, хто має непрямий контроль або значний інтерес, через поріг в 5 %; громадянство/статус перебування осіб з більш 5 % акцій; країна місцезнаходження компанії з більш ніж 5% акцій; ідентичність реальних власників, де акції проводяться від імені іншої особи, наприклад, за допомогою брокерських компаній. Крім того, з метою виявлення потенційних джерел впливу на медіа-контент, важливо, що медіа-компанії мають бути зобов'язані публікувати фінансову звітність та аудиторські звіти, підготовлені відповідно до найвищих міжнародних стандартів;

2) інформація легко доступна та безкоштовна;

3) інформація має регулярно оновлюватися (протягом 10 робочих днів з дня зміни структури власності);

4) дані мають бути доступні для повторного використання у відкритих форматах;

5) прогресивне збільшення прозорості. Країни, що забезпечили прозорість щодо основної інформації повинні рухатися до більшої прозорості через обов'язкове розкриття інформації про власників з більш ніж 5 % акцій в медіа-компаній;

6) прозорість впливу. Для того, щоб зрозуміти більш докладно не тільки, хто володіє, але й того, хто контролює засоби масової інформації, також потрібно розкривати наступну інформацію: вище керівництво, наприклад, директори (фірми), ключові посадові особи виконавчих органів, відповідальні редактори; деталі щодо голосування, де вони не в рівній мірі розподілені між акціонерами, включаючи записів голосування на загальних зборах;

7) чиста та точна юридична база. Положення, що стосуються розкриття інформації про власність на засоби масової знаходяться в одному законі, що регулює суспільні відносини стосовно аудіовізуальних, друкованих та нових медіа;

8) нагляд з боку незалежного органу. Незалежний наглядовий орган, до повноважень якого належить реєстрація аудіовізуальних засобів масової

інформації, має бути уповноважений і наділений достатніми ресурсами для моніторингу та забезпечення дотримання відповідного законодавства;

9) безпосереднє розкриття інформації громадськості. Засоби масової інформації повинні бути зобов'язані розкривати безпосередньо до громадськості ту ж інформацію, що надається до національного регуляторного органу;

10) транснаціональний доступ і порівнянність. Європейський Союз і Рада Європи повинні доповнювати національну прозорість механізмів власності на засоби масової інформації, досліджуючи систему, за допомогою якої дані, зібрані на національному рівні для всіх трьох секторів засобів масової інформації (аудіовізуальні, друковані та нові медіа) будуть систематизовані і загальнодоступні.

Результати аналізу чинного законодавства щодо прозорості власності на засоби масової інформації на відповідність рекомендаціям Access Info Europe, на нашу думку, не втішні.

Протягом останніх трьох років Верховною Радою України прийнято три закони, спрямовані на виконання зазначених зобов'язань Україною, а саме:

«Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації» від 4 липня 2013 р. № 409-VII [5];

«Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» від 14 жовтня 2014 р. №1701-VII [6];

«Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення» від 3 вересня 2015 р. № 674-VIII [7].

Не зважаючи на це, наразі відсутня будь-яка достовірна інформація щодо того, кому належать українські аудіовізуальні засоби масової інформації.

Однією з основних позитивних новел прийнятого у 2013 р. Закону України «Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації» [5] було те, що право аудіовізуальних засобів масової інформації як суб'єкта господарювання на надання інформації про свого власника у відповідь на запит стало обов'язком [8]. Проте, Закон отримав багато критики з боку медіа спільноти та представників засобів масової інформації.

Закон України «Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» [6] також регулював питання прозорості відносин власності щодо аудіовізуальних засобів масової інформації. Законом передбачено подання юридичними особами державному реєстратору інформації про структуру власності засновників, відомостей про свого кінцевого вигодоодержувача (вигодоодержувачів) у тому числі кінцевого

вигодоодержувача (вигодоодержувачів) їх засновника, якщо засновник – юридична особа.

Проте, зазначені положення Закону суб'єкти законодавчої ініціативи визнали недостатніми для належного забезпечення права кожного на інформацію про власників аудіовізуальних засобів масової інформації і 3 вересня 2015 р. Верховною Радою України було прийнято Закон України «Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення» [7].

Слід зазначити, що після прийняття цього спеціального Закону суспільні відносини щодо забезпечення прозорості відносин власності стосовно аудіовізуальних засобів масової інформації вже не регулюються Законом України «Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів» [6]. Тобто, працюватиме правило про співвідношення загальної та спеціальної норм.

Вказаним Законом статтю 1 Закону України «Про телебачення і радіомовлення» доповнено новими визначеннями. Нашу увагу привернуло визначення терміну «публічна компанія», згідно з яким це юридична особа, створена у формі публічного акціонерного товариства, акції якої включені до біржових списків (пройшли процедуру лістингу) фондових бірж, що відповідають критеріям, визначеним Національним банком України. При цьому, вважається, що публічна компанія не має осіб, які мають істотну участь, здійснюють над нею контроль, та є такою, що не має кінцевого бенефіціарного власника (контролера). У результаті цього фактично дія Закону України «Про телебачення і радіомовлення» щодо визначення структури власності не поширюватиметься на публічні компанії. Таким чином, цим Законом прямо передбачено можливість не надавати інформацію про реальних власників аудіовізуальних засобів масової інформації, якщо їх засновником є публічна компанія.

На нашу думку, сьогодні край необхідно врахувати кращі європейські практики організаційно-правового забезпечення державної інформаційної політики щодо прозорості відносин власності стосовно аудіовізуальних засобів масової інформації, оскільки їх діяльність впливає на інформаційну безпеку нашої країни в цілому.

З огляду на наведене, у новій редакції Закону України «Про телебачення і радіомовлення» необхідно передбачити ефективний механізм обмеження щодо монополізації телерадіоорганізацій промислово-фінансовими, політичними та іншими групами чи окремими особами.

Література

1. Про телебачення і радіомовлення : Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 2006. – № 18. – ст. 155. –

[Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3759-12.

2. Про виконання обов'язків та зобов'язань Україною : Резолюція Парламентської Асамблеї Ради Європи від 5 жовтня 2005 р. № 1466. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_611.

3. Who really owns the media? You have a right to know! – [Електронний ресурс]. – Режим доступу : http://www.access-info.org/media-ownership-transparency.

4. Ten Recommendations on Transparency of Media Ownership. Access Info Europe & OSPIJ, 4 November 2013. – [Електронний ресурс]. – Режим доступу : http://www.access-info.org/tmo/12338.

5. Про внесення змін до деяких законів України щодо забезпечення прозорості відносин власності стосовно засобів масової інформації : Закон України від 4 липня 2013 р. № 409-VII // Відомості Верховної Ради України. – 2014. – № 20-21. – ст. 715. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/409-18.

6. Про внесення змін до деяких законодавчих актів України щодо визначення кінцевих вигодоодержувачів юридичних осіб та публічних діячів : Закон України від 14 жовтня 2014 р. №1701-VII // Відомості Верховної Ради України. – 2014. – № 46. – ст. 2048. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1701-18.

7. Про внесення змін до деяких законів України щодо забезпечення прозорості власності засобів масової інформації та реалізації принципів державної політики у сфері телебачення і радіомовлення : Закон України від 3 вересня 2015 р. № 674-VIII. – [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/674-19.

8. Беляева К. В. Европа на страже прозрачности украинских СМИ // Судебно-юридическая газета, 2013. – № 33 (201). – [Електронний ресурс]. – Режим доступу : http://sud.ua/newspaper/2013/08/23/53506-evropa-na-strazhe-prozrachnosti-ykrainskikh-smi.

ОПТИЧЕСКИЕ НОСИТЕЛИ ИНФОРМАЦИИ С ПОЛЯРИЗАЦИОННЫМ ШИФРОВАНИЕМ ДАННЫХ

А.А. Крючин, Е.В. Беляк, Е.М. Морозов
Институт проблем регистрации информации НАН Украины

Введение

Оптические носители информации имеют большие потенциальные возможности для долговременного хранения информации. Кроме обеспечения высокой стабильности свойств при изменении условий хранения носителей оптические носители предоставляют условия для шифрования записываемой информации. Шифрование записываемой информации на оптических носителях наиболее эффективно реализуется на носителях с многоуровневым представлением записываемой информации. Применение многоуровневых систем регистрации информации позволяет решить две задачи: существенно повысить плотность записи информации без увеличения разрешающей способности фокусирующих систем и повысить уровень защиты от несанкционированного доступа. Носители с многоуровневым представлением информации могут создаваться с применением различных способов записи и на основе различных материалов. Одним из вариантов многоуровневого носителя может быть носитель, регистрирующая среда которого выполнена из смеси красителей, каждый из которых обесцвечивается при экспонировании излучением с различными длинами волн [1-3]. Реализовать многоуровневое представление записанной информации можно на носителях, регистрирующие среды которых селективно взаимодействуют с электромагнитным излучением с различной поляризацией. Такие носители информации не только позволяют записывать информацию с большей плотностью при использовании системы записи с одинаковой разрешающей способностью, но и шифровать информацию, которая регистрируется на оптическом носителе. Информация может быть зашифрована с использованием определенного поляризационного состояния записывающего луча, и не может быть считана без предварительного знания ключа поляризации. Поляризованное излучение может селективно взаимодействовать с оптическими материалами с анизотропными свойствами. Изменение характеристик оптических материалов в значительной степени зависит от ориентации электрических диполей с учетом поляризационных состояний света. Информация может быть зашифрована с использованием определенного поляризационного состояния записывающего пучка, которая не может быть считана без предварительного знания ключа поляризации. При изменении поляризации несколько блоков информации могут быть зашифрованы в той же пространственной области с различным ключом поляризации. Введение

дополнительных параметров в технологию записи информации на оптический диск несет в себе новые возможности для шифрования данных. Можно использовать комбинации как минимум 10 различных паттернов при записи данных на оптический носитель, и при этом лишь те пользователи, кто знает правильный цвет и поляризацию, смогут выбрать правильный паттерн для чтения [1-5]. Возможности шифрования данных на оптических носителях с использованием поляризационного шифрования, голографического представления данных, 3D-ориентированных поляризационных состояний, технологии оптической записи с использованием угловых моментов представлены на рис. 1 [1, 4].

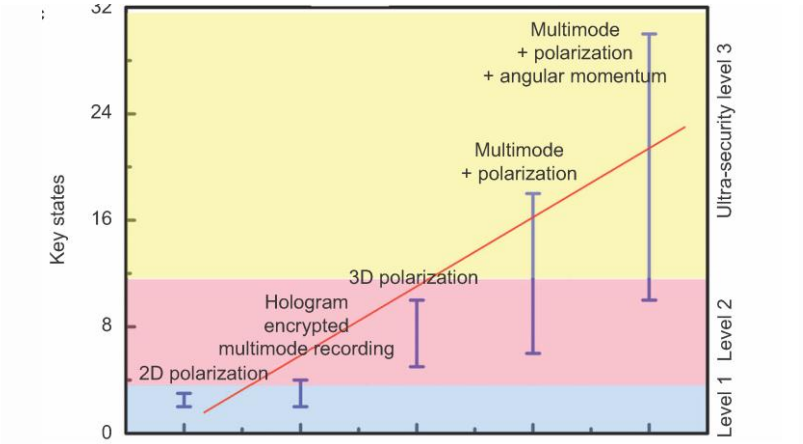


Рис. 1. Схема шифрования данных на оптических носителях с использованием различных методов записи и считывания информации оптическим излучением, в том числе с оптическим поляризационным мультиплексированием [1, 4]

Наибольший уровень криптографической защиты обеспечивается при комплексном использовании перечисленных методов. Следует отметить, что поляризационное мультиплексирование достаточно широко используется в современных системах передачи данных для повышения скорости передачи информации. Поляризационное мультиплексирование позволяет удвоить скорость передачи данных без расширения полосы сигнала. Увеличение скорости достигается за счёт создания передатчиком двух потоков, работающих в одной полосе, но на ортогональных поляризациях (вертикальной и горизонтальной) [6].

Технология поляризационного мультиплексирования в системах оптической записи

Поляризационное мультиплексирование основано на использовании поляризационного лазерного излучения для записи нескольких отдельно адресуемых битов в одном и том же объеме. Для достижения поляризационного мультиплексирования требуются фоточувствительные материалы, которые обладают чувствительностью к поляризации оптического излучения. Фотохромные красители являются такими соединениями и широко используются для поляризационного кодирования. Поляризационное кодирование достигается за счет оптически индуцированного двулучепреломления в фотохромных красителях за счет фотоизомеризации. Технология поляризационного мультиплексирования позволяет производить запись различных информационных массивов в одной области носителя информации. Схема процесса поляризационной записи представлена на рис. 2 [7].

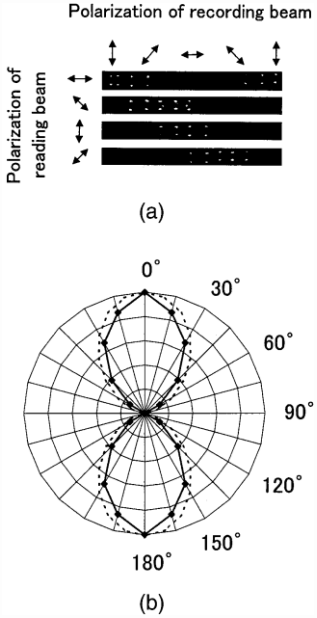


Рис. 2. Запись и чтение с разными направлениями поляризации: (а) считывание информационных единиц, записанных с помощью поляризационного излучения с углом поляризации от 0° до 180° с шагом 15°; (б) поляризационное считывание данных [7].

Регистрирующие среды для поляризационного мультиплексирования

В последние десятилетия были предложены многочисленные многоуровневые оптические методы записи информации, основанные на использовании излучения с различными длинами волн и поляризацией. Однако отсутствие необходимых регистрирующих сред препятствовало достижению существенного увеличения информационной емкости. Поляризационно селективные регистрирующие среды могут создаваться с использованием различных эффектов. В одной из первых работ использовались сополимеры urethane-urea (уретана мочевины). Боковые цепи сополимеров urethane-urea вызывают цис-транс изомеризацию при освещении синим или зеленым светом, и они присоединяются перпендикулярно направлению линейной поляризации освещаемого света, что приводит к появлению оптической анизотропии. Было обнаружено, что полученный материал обладает селективной анизотропией в определенном направлении, что позволило записать три различных блока данных в одной области носителя информации, было также продемонстрировано стирание записанных данных (рис. 3) [7].

Развитие нанотехнологий открывает новые возможности управления свойствами материалов на нанометровом уровне, что может обеспечить новые подходы для реализации более надежного и безопасного хранения данных на оптических носителях. Использование для представления информации голографической записи, комплекса различных характеристик фоточувствительного материала, таких как поляризационные характеристики, значений угловых моментов, позволяет достичь более высокого уровня информационной безопасности при хранении данных на оптических носителях по сравнению с побитовым представлением данных. Достижение высокого уровня безопасности хранения данных сильно зависит от свойств материала носителя записи, в частности, его детерминированной реакции на свет с различными характеристиками [1]. Поляризационно селективные регистрирующие среды могут создаваться на основе использования уникальных свойств продольного поверхностного плазмонного резонанса (SPR) в золотых наностержнях [7]. Золотые наностержни представляют собой кластеры цилиндрической формы, размер которых составляет менее 100 нм. Электроны проводимости в золоте могут свободно перемещаться в пределах наностержней.

При совпадении частоты светового излучения с частотой коллективных собственных колебаний электронов в золотом наностержне возникает явление поверхностного плазмонного резонанса (surface plasmon resonance, SPR), которое приводит к сильному взаимодействию наностержня с электромагнитным полем света. В результате золотые наностержни обладают сильным поглощением в узком диапазоне длин волн. Запись на регистрирующей среде из наностержней осуществляется фемтосекундными лазерными импульсами в полосе поглощения наностержней.

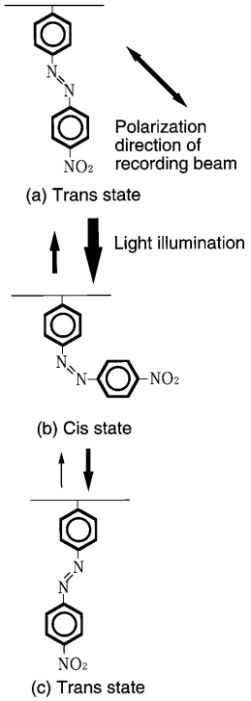


Рис. 3. Механизм анизотропной поляризационной записи на основе фотоизомеризации уретан-мочевинного сополимера [7]

При достаточной мощности лазерного излучения происходит расплавление стержней при температуре ~1000 °С, и превращение их в сферические частицы, что изменяет их спектр поглощения, что, в свою очередь, проявляется в изменении цвета. Золотые наностержни чувствительны к длине волны экспонирующего излучения. Под действием излучения с различными длинами волн расплавляются наностержни с определенным соотношением длины и ширины, что приводит к появлению поглощения на других длинах волн (рис. 4).

Поляризованное лазерное излучение плавит только те золотые наночастицы, расположение которых соответствует определенному направлению поляризации. Проведенные эксперименты показали, что золотые наностержни, диспергированные в поливинилхлоридную пленку, были преобразованы в сферические частицы при импульсном облучении (1064 и 532 нм). При облучении линейно поляризованным лазерным излучением наблюдается индуцированное селективное преобразование

наностержней, в результате которого изменяются дихроичные свойства пленки. Степень преобразования зависит от длины волны, а также от направления поляризации лазерного луча [9].

Мультиплексирование возможно за счет использования оптических свойств наностержней, которые позволяют селективно возбуждать и плавить только наностержни с определенным соотношением длины и диаметра при различной поляризации света. Наностержни других размеров не подвержены влиянию лазерного луча, и могут быть использованы для записи других информационных блоков. При изготовлении носителей информации наностержни размещают в инертной матрице. В качестве материала матрицы предлагалось применять стекло, которое выдерживает высокие температуры, которыми обладают золотые наностержни в процессе записи. К сожалению, сложно подобрать растворители для приготовления стеклянной матрицы, с которыми не взаимодействуют наностержни. В целях предотвращения агрегации наностержней могут применяться полимерные матрицы, однако полимеры имеют низкие температуры деструкции, что оказывается критическим при фототермическом способе записи.

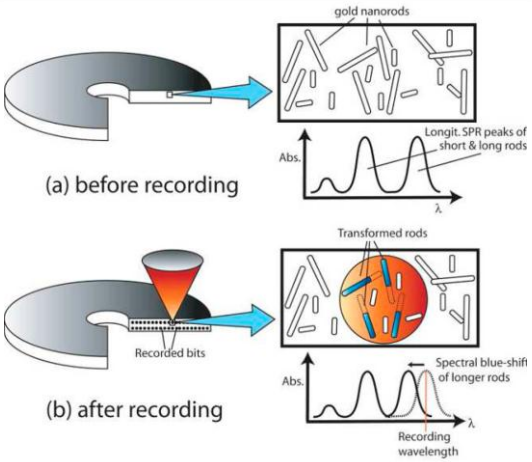


Рис. 4. Спектральное мультиплексирование с использованием золотых наностержней. Узкие полосы поглощения наностержней позволяют избирательно возбуждать и изменять характеристики стержней только определенного размера. Стержни других размеров остается неизменными и могут быть использованы для записи другого информационного блока [3]

Явление поверхностного плазмонного резонанса приводит к сильному взаимодействию золотых наностержней со светом определенной длины, которое зависит от формы, размера и ориентации частиц. Анизотропная

форма золотых наностержней вызывает расщепление поверхностного плазмонного резонанса (SPR) на поперечную и продольную компоненты, из которых последняя наблюдается в ближнем инфракрасном диапазоне длин волн и является чрезвычайно чувствительной к длине волны и поляризации падающего света. Продольная компонента поверхностного плазмонного резонанса (SPR) в золотых наностержнях характеризуется сильным поглощением света, что делает их идеальным фототермическим преобразователем энергии. Уникальной особенностью наностержней является зависимость поглощения света от ориентации частиц по отношению к поляризации света. На рис. 5 показано коэффициент поглощения для частиц, которые ориентированы параллельно (пунктирная линия) и перпендикулярно (сплошная линия) к поляризации падающего света. Когда частица находится на линии, параллельной поляризации падающего света, наблюдаются продольные полосы поглощения. Когда наностержни ориентированы перпендикулярно поляризации света, наблюдается слабый поперечный резонанс на длине волны около 530 нм, как и для сферических частиц. На рис. 5 (б) показаны рассчитанные значения коэффициента поглощения зависимости от угла поляризации, наностержень при этом моделируется сфероидом. Угловое распределение поглощения имеет косинусную зависимость, которое характерно для идеального диполя.

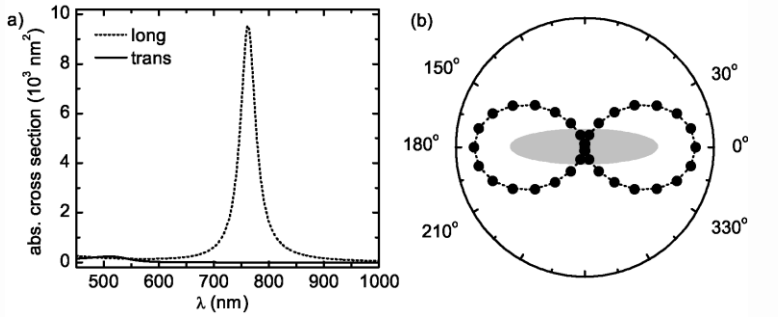


Рис. 5. Рассчитанные коэффициенты поглощения в зависимости от ориентации наностержней (а): коэффициенты поглощения наностержней в зависимости от поляризации падающего света. Длина большой полуоси составляет 25 нм, а длина малой полуоси составляет 7,5 нм, наностержни были помещены в среду с показателем преломления ε = 2,25; (б) величина поглощения в зависимости от линейной поляризации света в максимуме продольного поверхностного резонанса SPR. Ориентация наностержня относительно поляризации света представлена в центре графика в полярной системе координат [9]

SPR позволяет создавать регистрирующие среды, которые обладают селективностью к длинам волн и поляризации, в то время как явно выраженный энергетический порог, необходимый для фототермической записи, обеспечивает механизм осевой избирательности. Считывание осуществляется с помощью SPR опосредованной двухфотонной люминесценции, которая обладает повышенной спектральной и угловой селективностью по сравнению с обычными линейными механизмы обнаружения. Двухфотонная люминесценция позволяет осуществлять неразрушающее считывание с минимальным уровнем перекрестных помех.

Выводы

1. Поляризационное мультиплексирование используется не только для увеличения емкости оптических носителей, но и как универсальное средство для шифрования информации для защиты данных, которое является одним из наиболее важных аспектов функционирования любой системы памяти.
2. Основная проблема создания систем оптической памяти с поляризационным мультиплексированим является получение фоточувствительных материалов, которые обладают свойством поляризационной селективности.
3. Поляризационно селективные регистрирующие среды могут создаваться на основе продольного поверхностного плазмонного резонанса в золотых наностержнях, которые могут быть применены для создания оптических носителей информации со сверхплотной записью и возможностью шифрования данных.

Литература

1. Gu M. Optical storage arrays: a perspective for future big data storage / M. Gu, X. Li, Y. Cao // Light: Science & Applications. – 2014. – Vol. 3: e177.
2. A multidye nanostructured material for optical data storage and security data encryption / H.H Pham, I. Gourevich, J.K. Oh [et al.] // Adv. Mater. – 2004. – Vol. 16. – P. 516–520.
3. Zijlstra P. Photothermal properties of gold nanorods and their application to five-dimensional optical recording: doctoral thesis / Peter Zijlstra. – Centre for Micro-Photonics Faculty of Engineering and Industrial Sciences Swinburne University of Technology Melbourne, Australia, 2009. – 149 p.
4. Gu M. Plasmonic keys for ultra-secure information encryption / M. Gu, X. Li, T.H. Lan, C.H. Tien // SPIE Newsroom. – 19 November 2012. – doi:10.1117/2.1201211.004538.
5. Rewritable polarization-encoded multilayer data storage in 2,5-dimethyl-4-(*p*-nitrophenylazo)anisole doped polymer / X. Li, J.W. Chon, S. Wu [et al.] // Opt. Lett. – 2007– Vol. 32. – P. 277–279.

6. Обзор способов повышения производительности радиорелейных линий связи / Е. В. Рогожников, Е. П. Ворошилин, А. С. Колдамов, А. А. Гельцер // Вестник СибГУТИ. – 2013. – №4. – С. 3–11.

7. Polarization-multiplexed optical memory with urethane-urea copolymers / S. Alasfar, M. Ishikawa, Y. Kawata [et al.] // Appl. Opt. – 1999. – Vol. 38. – P. 6201–6204.

8. Zijlstra P. Five-dimensional optical recording mediated by surface plasmons in gold nanorods / P. Zijlstra, J. Chon, M. Gu // Nature. – 2009. – Vol. 459(7245). – P. 410–413.

9. Dichroism of poly(vinylalcohol) films containing gold nanorods induced by polarized pulsed laser irradiation / Y. Niidome, S. Urakawa, M. Kawahara, and S. Yamada // Jpn. J. Appl. Phys. – 2003. – Vol. 42. – P. 1749–1750.

ПИТАННЯ ЯКОСТІ, КОНФІДЕНЦІЙНОСТІ ТА КОРЕКТНОСТІ ДАНИХ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ АНАЛІЗУ ФІНАНСОВИХ РИЗИКІВ

Кузнєцова Н.В.
Навчально-науковий комплекс «Інститут прикладного системного аналізу» НТУУ «КПІ»

Системи ризик-менеджменту, що розробляються для розв'язання задач оцінювання та прогнозування фінансових ризиків, характеризуються опрацюванням даних, що надходять в реальному часі, та необхідністю приймати рішення та здійснювати управління в той же момент часу. До інформації, яка передається в інформаційну систему, висуваються вимоги щодо значущості, повноти, достовірності, своєчасності, зрозумілості, релевантності, співставленості та ефективності. Своєчасність передачі інформації може бути забезпечена за рахунок використання сучасних інструментів та швидкісних каналів передачі, періодичного оновлення показників (наприклад, кожен день оновлюється курс валют у системі) тощо. Значущість вхідної інформації суттєво впливає на результаті прийняття фінансових рішень та формування фінансової стратегії підприємства. Повнота та достовірність інформації суттєво залежить від джерел вхідної інформації, від коректності показників, що використовуються, від того, наскільки отримана інформація адекватно відображає реальний стан і результати фінансової діяльності, незаангажована по відношенню до усіх потенціальних користувачів, та найголовніше, коректна та перевірена. Інформаційні технології фінансового ризик-менеджменту ґрунтуються на статистичних та математичних методах і спрямовані на автоматизовану обробку даних. Тож питання безпеки та захищеності даних постають на всіх етапах організації збору та аналізу фінансових даних (рис. 1).

Перший етап зазвичай реалізується компаніями за допомогою чіткої організаційної структури філіалів, офісів, торгівельних представників, дилерів, тощо. У подальшому надану інформацію будемо називати *інформацією з «полів»*.

Організації на місцях збирають статистичну інформацію у вигляді затвердженої звітності про фінансові показники компанії, рівні продажів, фінансовий стан (платоспроможність) та дані клієнтів (збираються банками). Зазвичай у всіх установ є свої однотипні форми звітності: форми, анкети, бланки, які заповнюються працівниками у «полях», а потім передаються у вигляді електронного файлу.

Частина полів у файлі має бути недоступною для редагування користувачами на місцях (наприклад, порядок та назви полів форм), а частина полів має бути відкрита для введення інформації з «полів». На

цьому етапі обов'язково має бути перевірена та проконтрольована правильність та коректність введення даних.

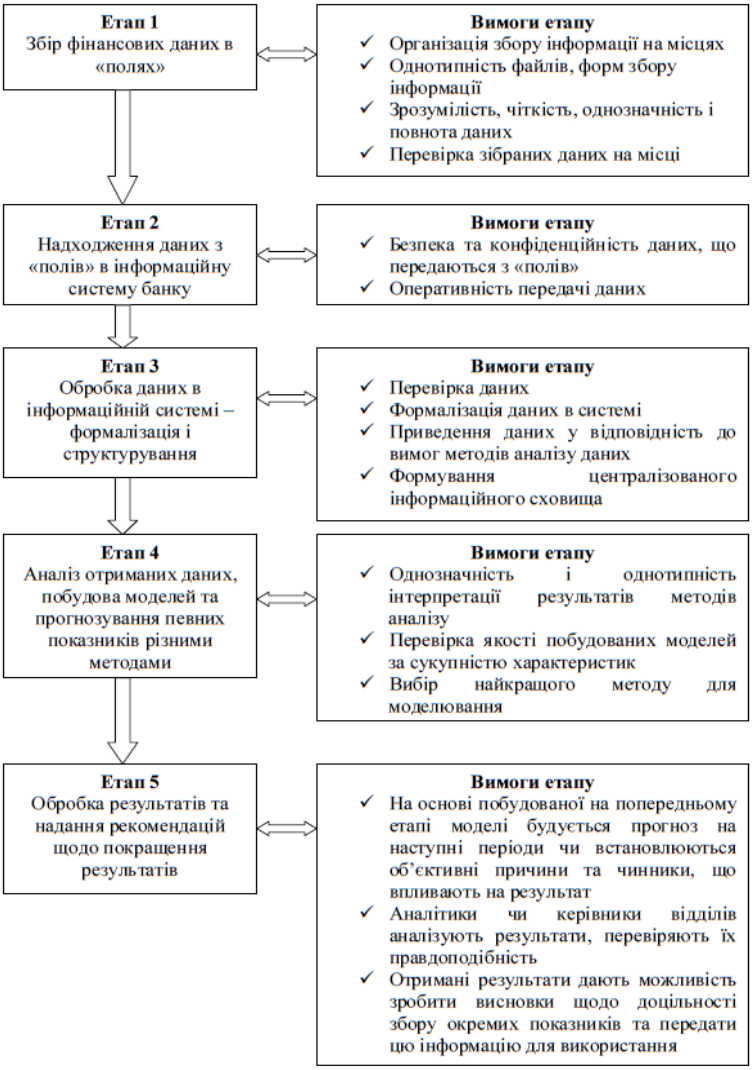


Рис. 1. Організація процесу аналізу фінансових даних

На *другому етапі* необхідно забезпечити збереження конфіденційності інформації, неможливість втручання сторонніх осіб у процес передачі даних. Ще однією вимогою етапу є оперативність передачі інформації до центрального офісу. Частина фінансових даних збирається при роботі з клієнтами, тому час очікування клієнта має буде зведений до мінімуму.

На *третьому етапі* здійснюється обробка даних, що надійшли з підрозділів, перевірка коректності та повноти цих даних, приведення їх до однотипного формалізованого вигляду, передача у централізовану систему збереження інформації – інформаційне сховище (або базу даних) [1,2]. Частина даних може зберігатися у базах даних (БД), доступ до яких здійснюється через інтегровані програмні продукти, такі як SAP, SAS, Nielsen чи на сервері, звідки дані можуть бути легко вивантажені у зручній формі, наприклад в електронний документ Excel.

На *четвертому етапі* наявні підготовлені для аналізу дані. Використовуються доступні методи аналізу даних (логістична регресія, дерева рішень, нейронні мережі, мережі Байєса, тощо) та будується модель. Перевіряється адекватність моделі за різними якісними характеристиками, наприклад, загальна точність, помилки 1-го та 2-го роду. Серед побудованих моделей обирається краща [2, 3].

На *п'ятому етапі* відібрані моделі аналізу даних використовуються для обчислення прогнозних оцінок. Для уточнення оцінок рекомендується комбінувати прогнози, отримані за декількома моделями. Аналітики та керівники відділів надають висновки і рекомендації щодо адекватності отриманих результатів, доцільності збору та використання певних показників на етапі побудови та використання моделі.

Отже, нагромаджуються великі обсяги даних, які на четвертому та п'ятому етапі наведеної на рис. 1.1 схеми мають бути ретельно оброблені згідно з вимогами користувачів. Якщо на перших трьох етапах дані структуруються вже за рахунок введення раціональної структури бази даних, то четвертий та п'ятий етапи потребують спільних зусиль експертів, аналітиків і керівників підприємств.

Прикладом спеціалізованого інструменту для спрощення процесу аналізу даних при створенні інтелектуальних та описових модулів, основаних на великих обсягах даних підприємства, може бути *SAS Enterprise Miner*. Інструмент містить широкий набір методів ІАД – регресійний аналіз, дерева рішень, нейронні мережі, машина опорних векторів, кластерний аналіз та багато інших спеціалізованих та надсучасних методів. Інструмент використовується для розв'язання задач аналізу шахрайства, мінімізації ризиків, прогнозування потреб у ресурсах, зменшення часу простою активів, збільшення ефективності маркетингових кампаній, запобігання відтоку клієнтів, розробки скорингових карт, збільшення продажів товарів тощо [4, 5].

Застосування SAS Credit Scoring for Banking для протидії шахрайству

Можливості інформаційної технології аналізу фінансових ризиків програмного продукту Credit Scoring for Banking в основному зосереджені на розв'язання задач кредитного скорингу: аналізу клієнтів за різними розрізами характеристик, проведенні розрахунків для різних кредитних продуктів, різних задач скорингу, перерахунку скорингових карт без додаткових інвестицій, формування алгоритмів виявлення шахрайства, здійснення збору і перетворення даних, формування звітності.

У банківській діяльності, зокрема, шахрайство означає цілеспрямоване отримання кредиту з метою зумисного неповернення (Fraud). І, поряд з формуванням моделей оцінки кредитоспроможності позичальників та проведення попереднього скорингу (Application Score), моделей оцінки змін кредитоспроможності існуючих позичальників для проведення поведінкового скорингу (Behaviour Score), а також формування моделей оцінки ймовірності, суми і оптимального способу впливу на поганих позичальників проведення скорингу по дефолту (Collection Scoring), необхідно розглядати формування моделей виявлення шахрайства для проведення скорингу шахрайства(Application Fraud Score).

Шахраїв можна розділити на три основні групи: «побутові» (індивідуали) шахраї; професійні шахраї; позичальники, які використовують послуги професіоналів-шахраїв (свідомо та несвідомо). «Побутові» шахраї не повертають кредит, оскільки не в змозі його повернути з матеріальних причин. Цей тип позичальників відноситься до малозабезпечених шарів населення, які повірили у рекламу і пізніше зрозуміли, що не можуть розраховуватися за кредит. Ці позичальники не будуть ховатися і змінювати адреси й телефони, але за судовим рішенням колектори і банк максимум, що з них отримають – це тіло кредиту. Такий тип позичальників попадає в «чорний список», заноситься до бюро кредитних історій, доступ до якого мають усі банки, і фактично банки більше не видадуть таким людям кредиту, а тому від них не постраждають.

Професійні шахраї, що проводять мобільний стиль життя, постійно змінюючи адресу проживання та регіон банків, змінюють телефоні номери, а іноді документи, надаючи неправдиву інформацію щодо місця своєї роботи, а фактично не працюючи ніде. Знайти їх складно, а тому страждає велика кількість банків, навіть консервативні банки, які вимагають довідку з місця роботи за офіційною формою податкової.

Третій тип позичальників – це ті особи, які свідомо використовують послуги шахраїв, розраховуючи отримані гроші вигідно вкласти, а після цього повернути кредит. Але часто це не вдається, і таким чином позичальник стає шахраєм.

Способом зниження кредитних ризиків шахрайства, особливо для беззаставних продуктів, є використання моделей виявлення шахрайства (Application Fraud Scoring). Застосування аналітичного модуля (інформаційної технології) SAS для формування таких моделей спрямовано

на допомогу банку створити послідовну і логічно підтверджену базу для прийняття рішень, надаючи співробітникам кредитного відділу більш чітку, інтуїтивно зрозумілу міру кредитного ризику. Модель скорингу фізичних осіб може базуватися на анкетних даних позичальників, експертних знаннях менеджменту банку, чисельних оцінках, отриманих за статистикою "поганих" і "добрих" кредитів, тощо. В результаті оцінки історичних даних (навчальній вибірці) формується кредитний портрет потенційного позичальника, що дозволяє проводити процедуру розподілу потенційних позичальників на "поганих" (шахраїв) та "добрих", яким кредит може бути видано. Цей результат закладається у навчальну вибірку цільової змінної (target) і будується модель і профіль шахрая (Scorecard Fraud).

Таким чином претенденти на отримання кредиту ранжуються по групах, кожній з яких присвоюється характеристика надійності позичальника від «високої» до «ризикованої»(шахрай). Аналіз кредитного скорингу (Score Fraud) дозволяє оцінити профіль шахрая і використати його на етапі прийняття рішення щодо видачі кредиту позичальнику. Після проведення оцінки на ймовірність шахрайства вже застосовуються традиційні моделі і скорингові карти для оцінки кредитоспроможності позичальника і ймовірності дефолту або прострочки.

Висновки

Найрізноманітніші інформаційні технології, які розроблені і призначені для аналізу фінансових ризиків, мають бути суттєво захищеними та неможливими для стороннього доступу як у процесі збору та передачі даних, так і на етапі прогнозування фінансових ризиків. Адже, якщо в процесі аналізу фінансових ризиків хоча б частина інформації буде спотвореною, це може суттєво вплинути на некоректне прогнозування того чи іншого ризику з портфелю фінансових ризиків, що повністю нівелює роботу всієї системи ризик-менеджменту. Особливо це питання стає актуальним при розробці інформаційних технологій для кредитного ризик-менеджменту, що працюють в реальному часі, і потребують захисту даних при введенні та передачі даних, а також бути застрахованими від роботи зловмисників. Для цього розробляють декілька видів скорингових карт, кожні півроку оновлюють скорингові моделі для унеможливлення підбору зловмисними «правильних» відповідей, моделюють профіль гарного клієнта та зловмисника, встановлюють профіль ризику, здійснюють варіацію порогу відсікання, аналізують відхилені заявки тощо. Всі ці дії спрямовані на підвищення обгрунтованності прийняття рішень та захисту структурних особливостей вибірок даних, на основі яких будується модель. При розробці інформаційних технологій, систем підтримки прийняття рішень основну увагу приділяють забезпечення безпеки та конфіденційності вхідних даних, своєчасності опрацювання та передачі даних з різних джерел, підбору коректних методів та моделей для оцінювання та прогнозування фінансових

ризиків, періодичне їх оновлення та застосування нових інтегрованих моделей, методів та підходів.

Література

1. Спирли Э. Корпоративные хранилища данных. Планирование, разработка, реализация / Эрик Спирли. – М.: Изд. дом Вильямс, 2001. – 396с.
2. Кузнєцова Н.В. Інформаційна технологія аналізу фінансових даних на основі інтегрованого методу / Н. В. Кузнєцова, П. І. Бідюк // Системні дослідження та інформаційні технології. – 2011. – № 1. – С. 22–33.
3. Бідюк П.І. Система підтримки прийняття рішень для аналізу фінансових даних / П. І. Бідюк, Н. В. Кузнєцова, О. М. Терентьєв / Наукові вісті НТУУ “КПІ”. – 2011. – №1. – С. 48–61.
4. Терентьев А.Н. SAS BASE: Основы программирования/ Терентьев А.Н., Домрачеев В.Н., Костецкий Р.И. – К.: Эдельвейс, 2014. – 304 с.
5. Siddiqi N. Credit risks scorecards. – New York: John Wiley & Sons, Inc., 2006. – 210 p.

МЕХАНІЗМИ ПІДВИЩЕННЯ ЖИВУЧОСТІ В СИСТЕМАХ ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ

Кузнєцова М.Г.
Інститут проблем реєстрації інформації НАН України

Організаційне управління являє собою неперервний процес напрацювання управлінських впливів і передачі їх підлеглим об'єктам управління для виконання і досягнення цілей організації. Системи організаційного управління (СОУ), підтримані певною інформаційною інфраструктурою, поєднують техніко-технологічний і соціальний аспекти виробничої діяльності і характеризуються наступними особливостями:

- можливість самостійного формування цілей і здатність до самоорганізації;
- необхідність урахування у процесі управління великої кількості політичних, соціальних та економічних факторів;
- висока невизначеність вхідних даних, неможливість прогнозування всіх факторів, які впливають на процес управління;
- низька ефективність використання математичних моделей для прийняття управлінських рішень;
- об'єктивний характер процесу управління і помилки при формуванні цілей і витрачанні ресурсів на їх досягнення через суб'єктивний людський фактор, оскільки основна роль при прийнятті рішень і організації управління, як правило, належить людині;
- велика кількість і різноманітність зв'язків та відносин між органами управління і окремими керівниками, відсутність чітких меж між керуючою системою і об'єктом керування, який до того ж має складну ієрархічну структуру.

СОУ являють собою складні ієрархічні системи з великою кількістю різнорідних елементів, взаємодіють із мінливим зовнішнім середовищем, мають цілеспрямовану поведінку, і повинні забезпечувати неперервність, сталість і безпеку функціонування для досягнення цілей організаційного управління. Сучасні СОУ підтримуються розвинутою інформаційною інфраструктурою [1], яка здатна забезпечити ефективність процесів обробки, передачі, зберігання та використання інформації, передбачає широке впровадження інформаційних технологій, використовує технічні і технологічні засоби автоматизації процесів управління, комп'ютерні засоби, бази даних і знань тощо.

Для СОУ актуальною є задача забезпечення інформаційної безпеки [2], враховуючи, що порушення процесів нормального функціонування інформаційної інфраструктури може призвести до порушень життєво значущих функцій. В інформаційній інфраструктурі сучасних СОУ, як правило, застосовуються засоби захисту інформації, визначено політику безпеки, впроваджено противірусні засоби тощо. Такі стандартизовані рішення

дозволяють розв'язати частину проблем із забезпечення інформаційної безпеки, але вони, як правило, добре відомі порушникам, до того ж і не завжди ефективно вирішують специфічні проблеми конкретної системи. Одним із перспективних підходів є використання механізмів підвищення живучості для протидії загрозам безпеці.

Інформаційна інфраструктура СОУ має кілька ієрархічних рівнів, на кожному з яких розв'язуються свої функціональні завдання [1]. Застосування механізмів підвищення живучості залежить як від функціональних завдань, що вирішуються, так і від наявних системних ресурсів.

Зазвичай виділяють наступні механізми підвищення живучості: розпізнавання, протидії, відновлення, адаптації, реконструкції, реконфігурації та реорганізації [3].

Механізми розпізнавання спрямовані на виявлення небезпечних станів чи спроб порушення функціонування системи (зокрема, виявляються атаки, успішні вторгнення, підвищення ризику виходу з ладу життєво значущих (критичних) компонентів систем, ризики втрати чи викривлення інформації). Реалізація механізмів розпізнавання потребує використання методів діагностики (відстеження небажаних відхилень у роботі системи та її компонентів); ідентифікації (присвоєння ідентифікатора об'єкту/суб'єкту системи чи перевірка відповідності між об'єктом/суб'єктом і його ідентифікатором); оповіщення (повідомлення користувачам чи відповідним структурам про небажані відхилення у роботі системи та її компонентів); реєстрації подій (збирання та зберігання інформації про дії та події); аналізу шаблонів ситуацій (порівняння послідовності дій та подій з відомими шаблонами атак і некоректного використання методів забезпечення надійності, відмовостійкості і безпеки, порівняння із шаблонами, напрацьованими під час сценарного аналізу).

Застосування механізмів протидії у СОУ спрямовано на підтримання визначених умов функціонування і мінімізацію збитків, які зумовлені переходом у нештатний режим функціонування. Аналіз можливих засобів та сценаріїв попередження реалізації таких загроз напрацьовується під час проектування або імітаційного моделювання створюваної СОУ. Для інформаційної інфраструктури СОУ такі механізми ґрунтуються на класичних методах забезпечення безпеки інформаційних систем: ідентифікації, авторизації, обмеженні привілеїв користувачів, встановленні технічних засобів протидії (наприклад, міжмережних екранів), введенні надмірності у систему (резервування апаратного і програмного забезпечення, створення архівів інформації).

Механізми відновлення мають забезпечити своєчасне реагування на небажані впливи, локалізувати їх наслідки і дозволити системі продовжити функціонування у непередбачених (нештатних) умовах. Стратегії відновлення для СОУ мають забезпечувати відновлення функціональності й працездатності компонентів та системи у цілому за небажаних впливів, а

також після їх припинення. Для відновлення інформаційної інфраструктури використовуються методи діагностики і цілий спектр спеціалізованих апаратно-програмних методів та засобів відновлення, що передбачають реплікацію критичних інформаційних ресурсів та сервісів, відмовостійкі архітектурні рішення, спеціалізовані засоби підтримання процесів відновлення, щоб гарантувати цілісність інформації або відновлення стану інформації за конкретних змін чи небажаних впливів.

Завдяки механізмам адаптації СОУ може цілеспрямовано змінювати параметри і структуру на основі інформації про зміни в умовах чи характері функціонування, виникнення непередбачених ситуацій, спрямоване порушення безпеки, а також про наслідки порушення безпеки. Ці механізми передбачають пристосування до нових умов роботи і максимізацію ефективності функціонування системи (зокрема, для інформаційної інфраструктури це може включати удосконалення засобів захисту та підсистем виявлення атак і реагування на них). Розробка та використання засобів та способів адаптації СОУ може виконуватись на основі аналізу ризиків та їх впливу на СОУ, бізнес-процеси та об'єкти управління; напрацьовані рішення можуть включати зміну параметрів функціонування системи, зміну функцій та навчання персоналу, розробку спеціальних технологій адаптивного керування в окремих ситуаціях за принципом «клас ситуацій - дії».

Механізм реорганізації забезпечує перерозподіл функцій компонентів системи, які вийшли з ладу, між працездатними компонентами або, у разі неможливості перерозподілу, – перехід системи до нової цілі функціонування.

Механізм реконфігурації реалізує автоматичну перебудову структури мережі обміну інформацією для досягнення найвищої ефективності виконання цілі функціонування за наявних працездатних ресурсів системи.

Механізм реконструкції виконує редукцію цілі функціонування та ресурсів системи до визначених базових рівнів, коли система може виконувати чітко окреслену множину функцій або забезпечити плавність деградації визначених параметрів.

Механізми живучості дозволяють ще до аналізу причин небажаної події зреагувати на небажаний вплив і забезпечити перехід системи у безпечний (заданий) для неї стан. Отже, спираючись на механізми забезпечення живучості, можна будувати системи, які будуть функціонувати з належною якістю в умовах небажаних впливів різної природи.

Впровадження тих чи інших механізмів забезпечення живучості у СОУ має обґрунтовуватися аналізом ризиків, урахуванням специфіки і функціонування кожної конкретної системи, урахуванням економічної складової.

Література

1. Додонов О.Г. Комп'ютерні засоби й інформаційні технології підтримки процесів управління реалізацією ділових процесів / Додонов

О.Г., Горбачик О.С., Кузнєцова М.Г. // Реєстрація, зберігання і обробка даних: зб. наук. праць за матеріалами Щорічної підсумкової наукової конференції 14-15 травня 2014 / НАН України. Інститут проблем реєстрації інформації, відпов. ред. В.В.Петров. – К.: ІПРІ НАН України, 2014. – С. 54-58.

2. Кузнєцова М.Г. Проблеми інформаційної безпеки в системах організаційного управління // Информационные технологии и безопасность. Основи обеспечения информационной безопасности: Материалы Международной науч. конференции ИТБ-2014. – В.14. – К.:ИПРИ НАНУ, 2014. – С. 50-56.

3. Додонов О.Г. Методологічні аспекти створення корпоративних інформаційно-аналітичних систем підвищеної живучості / Додонов О.Г., Кузнєцова М.Г., Горбачик О.С. // Реєстрація, зберігання і обробка даних, 2012. – № 3, Т.14. – С. 58- 69.

ОПТИМИЗАЦИОННОЕ МОДЕЛИРОВАНИЕ В EXCEL ЗАДАЧ О ПОТОКАХ В КОММУНИКАЦИЯХ

Кузьмичев А. И.
Институт проблем регистрации информации НАН Украины

Ключевое задание в обширной проблематике принятия решений – поиск критических составляющих («узких мест») в любой организационной структуре коммуникаций: технологических, транспортных, информационных и проч. Найденное «узкое место» – это гарантированное обеспечение минимальных затрат, связанных: для проектировщика или эксплуатационной службы – с совершенствованием параметров структуры, в частности, для сети, с поддержанием ее функциональности и живучести [1], для злоумышленника – с нанесением преднамеренного ущерба[1]. Чем большего размера и чем сложнее организована коммуникационная среда, тем труднее реализуется соответствующая потоковая задача поиска оптимума обобщенного показателя (продолжительность, стоимость, качество, риски) с учетом ресурсных ограничений.

Из-за огромного разнообразия специфических практических задач, сводимых к сетевой постановке, и предъявляемых требований к искомому решению, в теории графов выделен специальный аппарат сетевой оптимизации: теория сетей и потоков в них с собственным математическим аппаратом, классами специфических задач потокового программирования, оптимизационными методами и алгоритмами [2-5], специальными программными продуктами, литературой, а также учебными программами для новых профессий и специальностей.

Технология оптимизационного моделирования потоков в сетях, включая доступную и популярную среду электронных таблиц (*spreadsheets*) для ее реализации, – активная и распространенная составляющая этого аппарата [6, 7]. Истоки потокового моделирования и программирования: алгебраическая модель межотраслевых материальных потоков «затраты-выпуск» (В.В. Леонтьев, 1936 г.), линейное программирование: матричная модель транспортной задачи (Ф. Хитчкок, 1941 г., Л.В. Канторович, 1942 г.) и симплекс-метод (Дж. Данциг, 1949 г.), сетевые модели задач о потоках минимальной стоимости [8].

Живая практика демонстрирует уникальные ситуации, где решение классических сетевых задач имело весьма серьезные последствия, изменившие мир.

---

[1] Постановка задачи поиска минимального сечения сети – содержание секретного доклада (РЭНД, США) об эффективном методе разрушения железнодорожного сообщения между СССР и его странами-сателлитами с минимальными затратами ресурсов средств нападения, составленного в период «холодной войны» [8]

Пример 1 (глобальные сетевые коммуникации): решение частной задачи о поиске кратчайшего пути[2] в сети позволило указать «узкие места» в компьютерных сетях, чтобы осуществить поиск альтернативных маршрутов передаваемых пакетов в виде следующего кратчайшего пути, сформировав соответствующие протоколы обмена, аппаратное и программное обеспечения для массовых и разнообразных приложений сетевых коммуникационных технологий.

Пример 2 (организация, планирование и управление): из задачи о поиске кратчайшего пути вытекает, на первый взгляд странная, «зеркальная» задача о поиске длиннейшего пути в сети, но ее оригинальная постановка в виде сетевой модели проекта, решение на первых ЭВМ и успешное практическое использование (в конце 1950-ых гг.), привели к технологии сетевого моделирования проектов, последующему формированию и бурному развитию проектного менеджмента с массовой сферой приложений, со специальным ПО (типа *MS Project*), с образованием международных профессиональных организаций (*IPMA, PMI*) и стандартов (*PMBOK*), организацией научных конференций, открытием учебных и научных программ подготовки специалистов. В частности, в организации управленческой деятельности компаний активно развивается проектно-ориентированный менеджмент [ПОМ, 9] для принятия рациональных решений в условиях неизбежных, регулярных и частых изменений различной природы: норм и стандартов, требований к качеству готовой продукции, технологиям производства, свойств ресурсов, социально-политических, экономических и природных условий. Именно инструментарий оптимального планирования и управления проектами на основе их сетевых моделей обеспечивает успех ПОМ и его интенсивное применение в мировой экономике и бизнесе [10].

Пример 3 (микрокомпьютерная революция): формирование технологий и систем автоматизированного проектирования (САПР), в основе которых, в частности, для средств микроэлектроники, решение крупных и сложных оптимизационных сетевых задач, к которым сводится, например, трассировка печатных плат. Считается, что именно эти задачи вызвали стимулировали интерес и переход к практическому использованию теоретико-графовых моделей, к интенсивной и продуктивной разработке методов и алгоритмов сетевой оптимизации.

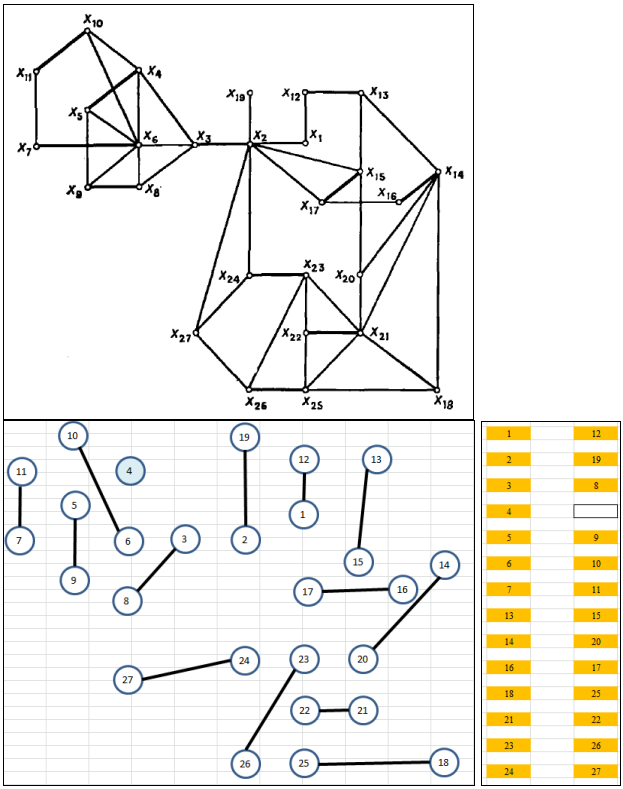
Типовые задачи о потоках в сетях

1) Паросочетания

«Узкие места» – удаленные связи между узлами.

Пример ($n = 27$, $m = 47$, все $c_j = 1$):

[2] A. Schrijver. On the History of the Shortest Path Problem in Documenta Mathematica, 2012. – p. 155-167



Варианты: о минимальном покрытии общего или двудольного графа, кластеризация.

2) Проектирование сетей, задачи о центрах и минимальных покрытиях

Проектирование сетевых структур выдвигает проблему рационального соединения отдельных узлов заданного множества в сеть определенного назначения в виде ее структуры, конфигурации и свойств. В рамках этой проблемы решены две задачи: о центрах и дереве минимального покрытия.

Задача о центрах – в коммуникационной системе выделяют весьма распространенный класс задач взаимодействия специальных узлов-центров с рядовыми узлами-клиентами (размещения и образования связей, *location-allocation*). В частности, в компьютерных сетях – это взаимодействие в рамках сетевой технологии «клиент-сервер». Различают задачи с одним или несколькими центрами, для оптимального размещения центров и

образования связей с узлами-клиентами используются типовые критерии оптимизации:

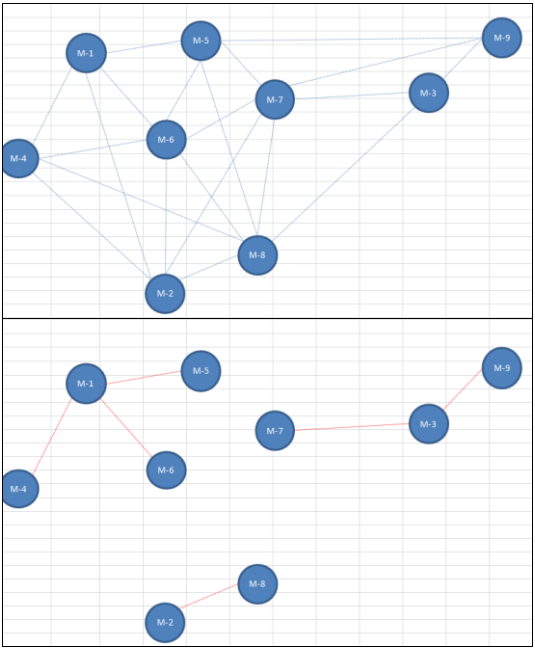
- *minsum* – для минимизации общих затрат на коммуникации,
- *maxmin* – для «плохих» центров или
- *minmax* – для «хороших» центров,

их комбинации и модификации (затраты на создание центров, радиус покрытия, логистические центры).

Дерево минимального покрытия – рациональное соединение всех узлов дугами, например, сотни узлов-скважин нефтяного месторождения дугами-дорогами с минимальной общей длиной или стоимостью сооружения, с использованием аналогичных критериев оптимизации и с учетом специальных условий.

Оптимизационных модели этих задач используют различные заданные и искомые параметры (время, стоимость, расстояние, надежность, качество, пропускная способность) и имеют свойства: статические/ динамические, линейные/нелинейные, одно/ многоуровневые, с принятием решений в условиях определенности/ неопределенности и проч.

Пример:

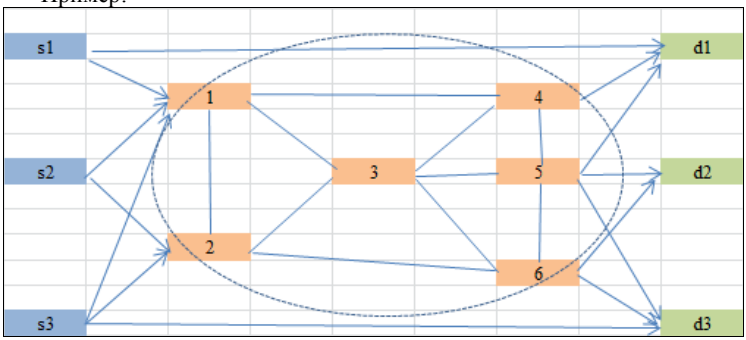


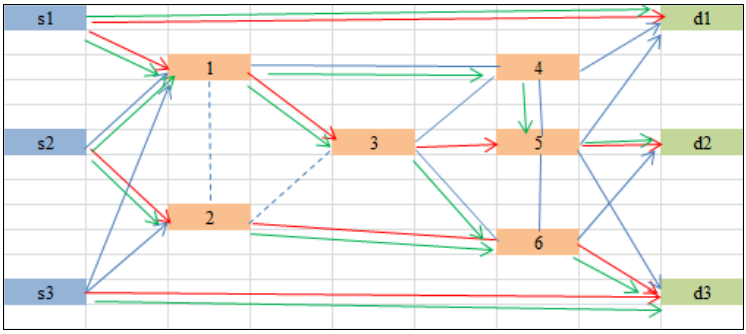
3) Задачи о потоках минимальной стоимости

Это:

- задачи транспортного типа в матричной или сетевой постановках
- задачи о назначениях
- одно- и многопродуктовые
- одно- и многополюсные.

Пример:



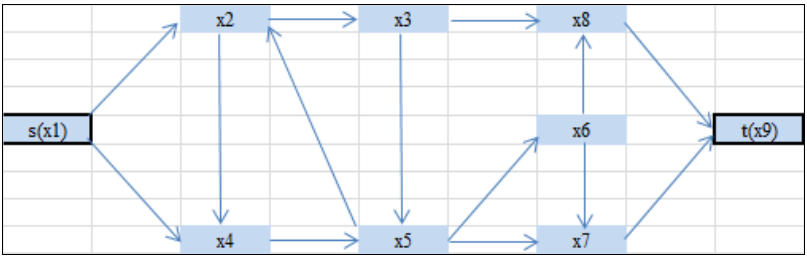


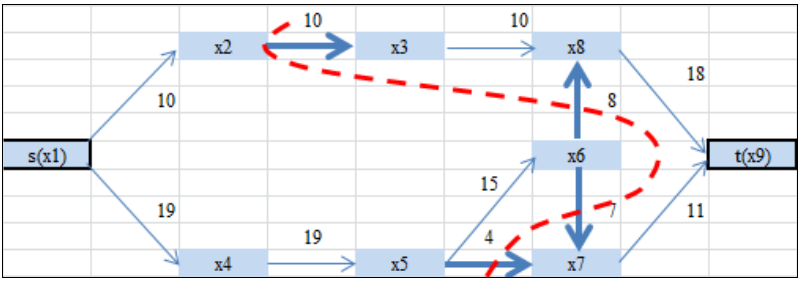
4) Задачи о максимальном потоке

Это потоки:

- в неориентированной, ориентированной и смешанной сети
- в двух- и многополюсных сетях
- одно- и многопродуктовые потоки
- с простыми и взвешенными узлами
- в обычных и мультиграфах.

Пример:





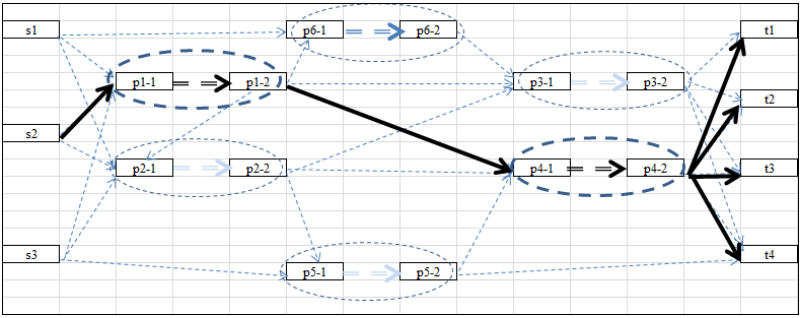
5) Потоки в обобщенных Δ-сетях

где Δ – коэффициент изменения величины потока на выходе из дуги (потери/прирост).

Это:

- максимальный поток
- максимально-оптимальный поток
- потоки с минимальными потерями
- активные (взвешенные) узлы.

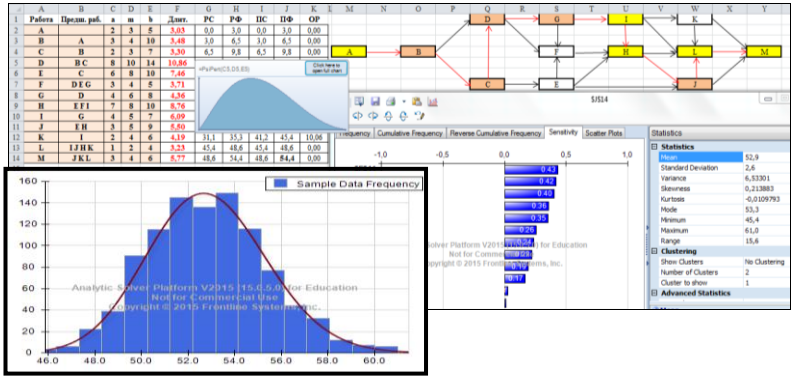
Пример:



6) Риск-анализ в сетевом моделировании проектов

Любой комплекс взаимосвязанных работ – это проект, который принято представлять соответствующей сетевой моделью (сетевым графиком) с параметрами: время, ресурсы, стоимость. Искомый результат: минимальная продолжительность с/без учета ресурсных или стоимостных ограничениях, минимальные дополнительные затраты для сокращения продолжительности и др. «Узкое место» – критические работы, требующие для своего своевременного исполнения особое внимание и дисциплину. Расчеты осуществляются в зависимости от специфики проекта и условий принятия решений – определенности (детерминированная модель)/неопределенности (вероятностная модель).

Пример вероятностной модели:



Литература

1. Фрэнк Г. Сети, связь и потоки/ Г. Фрэнк, И. Фриш: Пер. с англ. – М.: Связь, 1978. – 448 с.

2. Йенсен П. Потоковое программирование/ П. Йенсен, Д. Барнес: Пер. с англ. – М.: Радио и связь, 1984. – 392 с.

3. Evans J. Optimization Algorithms for Networks and Graphs/ J. Evans, E. Minieka. - Marcel, 1992. – 499 p.

4. Ahuja R. Network Flows: Theory, Algorithms, and Applications/ R. Ahuja, T. Magnanti, J. Orlin. – Prentice Hall. 1993. – 846 p.

5. Smith D. Networks and graphs: Techniques And Computational Methods/ D. Smith. – WP, 2003. – 225 p.

6. Baker K. Optimization Modeling with Spreadsheets/ K. Baker,2-ed. – Thomson, 2011. – 354 p.

7. Кузьмичов А.І. Оптимізаційні методи і моделі: Практикум в Excel/ А.І. Кузьмичов. – К.: АМУ, 2013. – 438 с.

8. Форд Л. Потоки в сетях/ Л. Форд, D. Фалкерсон.: Пер. с англ. – М.: Мир, 1962. – 275 с.
9. Turner R. The Handbook of Project-Based Management: Leading Change in Organizations/ R. Turner, 3-ed. – McGraw Hill, 2009. – 453 p.
10. Математические основы управления проектами. Под ред. В.Н. Буркова. – М.: Высш. шк., 2005. – 423 с.

АЛГОРИТМИ ПОБУДОВИ ОНТОЛОГІЇ НА ОСНОВІ ЗОНДУВАННЯ НАУКОВОЇ ЛІТЕРАТУРИ

Ланде Д.В., Прищепа С.В., Синькова Т.В.
Інститут проблем реєстрації інформації НАН України

Побудова великої галузевої онтології, як правило, складна науково-практична проблема [1], [2]. Основа цього процесу – побудова термінологічної основи і визначення деяких семантичних зв'язків [3].

Зондування наукометричної мережі

У рамках даної роботи розглядається метод побудови моделі предметної області (ПрО), заснований на знаннях, закладених у спеціалізованих текстах, що формуються фахівцями, експертами, авторами наукових праць.

Будемо розглядати зондуванням великих інформаційних мереж – таких, що з технологічних причин не підлягають повному скануванню, як вибірку невеликого обсягу найважливішого змісту. Для цього оберемо мережу тегів наукометричного сервісу Google Scholar Citations, вузли якої – поняття, марковані тегами, а ребра – деякі семантичні зв'язки між ними, обумовлені суміжними інтересами окремих авторів.

Як теги позначимо поняття наукового напрямку. Після введення відповідного тегу до адресного рядку, в інтерфейсі сервісу Google Scholar Citations у ранжируваному вигляді посторінково відображаються імена вчених, які позначили свої наукові інтереси заданим поняттям. Для кожного вченого вказані також інші поняття, що входять до сфери його наукових інтересів. Наприклад, для автора Piek Vossen визначені ще такі теги, як Lexical Semantics, Word-Sense-Disambiguation, Event Extraction, Text Mining, Knowledge Acquisition. Множина тегів-понять утворює мережу, похідну від біграфа «вчений-поняття» (біграф – це графа, множину вершин якого можна розбити на дві частини таким чином, що кожне його ребро з'єднує якусь вершину з однієї частини з якоюсь вершиною іншої частини). В рамках даної роботи як одну частину можна розглядати множину вчених, а іншу – множину тегів). Для моделі ПрО будемо розглядати похідну від цієї мережі, а саме мережу зв’язків окремих понять через авторів, яким ці поняття приписані. Очевидно, зв'язки такої «похідної» мережі можуть мати вагу, пропорційну кількості авторів, яким приписується відповідна пара понять.

Інколи, коли теги зазначені окремими вченими можуть належати до різних галузей науки, однак, попередньо проведені дослідження показують, що на невеликий, але досить репрезентативній вибірці (порядку сотні тегів), невелика частота нетематичних тегів забезпечує їх автоматичне «відсіювання» за деякім невеликим порогом.

Модель зондування мережі

Зондування модельної мережі здійснюється за принципом, подібним до того, що застосовується при пошуку інформаційних ресурсів в пірінгових мережах (від англ. Peer-to-peer, мережа – однорангова мережа, заснована на рівноправності учасників) [4], [5], [6].

Алгоритм зондування мережі Google Scholar Citations

Алгоритм, який застосовувався до модельних мереж, був адаптований до реальної мережі тегів сервісу Google Scholar Citations наступним чином:

1. Експертним шляхом визначається невеликий перелік базових тегів (ключових слів, відповідних найбільш важливим поняттями ПрО).
2. Вибирається тег із визначеного експертами переліку.
3. Відкриваються сторінки веб-сервісу, що відповідають цьому тегу (максимальна кількість таких сторінок параметрично обмежується заздалегідь).
4. До створюваної мережі додаються всі теги, що містяться на вибраних сторінках (сусідні теги).
5. Із сусідніх тегів вибирається той, на відповідні сторінки сервісу якого планується перейти для подальшого аналізу. Цей тег з найбільшим ступенем серед сусідніх тегів, який також задовольняє тематиці обраної ПрО і не входить до складу тих тегів, до сторінок яких вже було здійснено перехід.
6. Якщо такий тег обрано, то відбувається перехід до пункту 3.
7. Якщо такого тегу не існує, але перелік базових тегів не завершено, то здійснюється перехід до наступного базового тегу з початкового переліку, тобто перехід до пункту 2. У іншому випадку вважається, що мережа зондування побудована.

Процес зондування мережі, починаючи з певного вузла, припиняється при «зациклюванні», тобто коли відповідно до алгоритму відбувається перехід до вже пройденого тегу, а також при відхиленні від основної тематики сусідніх тегів, що залишилися.

Відхилення від основної тематики визначається експертами при автоматизованому зондуванні або з урахуванням лексичного складу тегів при повністю автоматичному скануванні. У разі автоматичного виконання алгоритму виконується обмеження за допомогою так званих «плюс-» і «стоп-словників» – наборів спеціальних шаблонів («плюс-» і «стоп-словник» в рамках даної роботи – набори шаблонів, підрядків, які повинні обов'язково входити або, відповідно, не входити в рядки, відповідні тегам). При цьому саме «зациклювання» є ознакою переходу до наступного базового тегу або завершення процесу зондування.

Експертами з ПрО виконується формування стартового переліку вузлів-понять і правил відбору «кінцевих» вузлів. Для побудови моделі ПрО (в розглянутому прикладі для області екстрагування подій із текстів)

експертним шляхом були визначені базові теги англійською мовою: Event Extraction; Information Extraction; Event Detection; Entity Extraction; Fact Extraction.

Як «плюс-словник» використовувався такий набір шаблонів: mining; event; extraction; entity; fact; monitoring; detection.

У розглянутому окремому випадку «стоп-словнику» відповідав набір шаблонів (зокрема, виключалася медико-біологічна тематика, туризм тощо): bio; medic; health; tourism; venture; portfolio; comparative.

При наведених вище трьох базових тегах, за результатами зондування мережі Google Scholar Citations, загальна кількість вузлів-тегів, які були екстраговані за алгоритмом, склала 148, у той час, як кількість нетермінальних вузлів – лише 14.

Приклад центрального фрагменту мережі понять ПрО, побудованої відповідно до наведеного алгоритму за вказаними базовим тегам наведено на рис. 3.

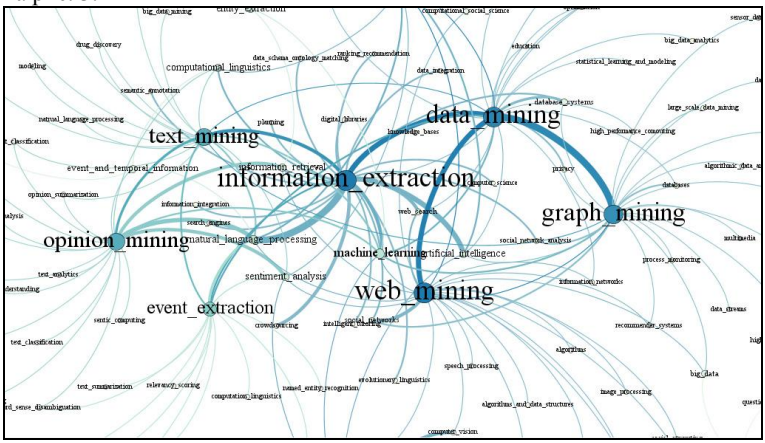


Рис. 3 – Центральний фрагмент мережі понять

Як видно з малюнка у цій мережі відбувся «зсув понять» (Topic Drift), тобто тег Event Extraction займає в ній далеко не центральне місце, яке природно займають такі більш поширені поняття, як Information Extraction, Data Mining, Web_mining. Разом з тим, саме місце поняття, що досліджується, у цій мережі, є необхідною якісною властивістю даної ПрО.

Побудова бібліографічних списків

На підставі побудованої в результаті зондування сервісу Google Scholar Citations мережі і можливостей даного сервісу реалізовано алгоритми автоматичного складання бібліографічних списків, що відповідають найбільш цитованим роботам у вибраній області за вказані проміжки часу.

Правила побудови бібліографічних посилань досить прості і охоплюють такі кроки:

1. Послідовно вибирається заздалегідь задана кількість найбільш вагомих вузлів побудованої мережі.
2. У відповідності з цими вузлами-тегами формуються запити до сервісу Google Scholar Citations і відбираються найбільш цитовані автори за вказаний період часу.
3. Відкриваються сторінки вибраних авторів, на яких наводяться посилання на публікації, із зазначенням їх цитування.
4. Серед найбільш цитованих робіт автора вибираються публікацій, заголовки яких відповідають «плюс-» і «стоп-словникам», приклади яких наведені вище.
5. У разі необхідності, з відібраних публікацій вибираються тільки ті, які містять посилання на повні тексти у форматі PDF.

На рис. 4 наведено приклад автоматично сформованого бібліографічного списку з посиланнями на PDF-файли публікацій.

Bibliography

1. *AnHai Doan.* Declarative information extraction using datalog with embedded extraction predicates. W Shen, AH Doan, JF Naughton, R Ramakrishnan. Proceedings of the 33rd international conference on Very large data bases..., 2007.: 152
2. *AnHai Doan.* Source-aware entity matching: a compositional approach. W Shen, P DeRose, L Vu, AH Doan, R Ramakrishnan. Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on..., 2007.: 161
3. *Andrew McCallum.* A comparison of event models for naive bayes text classification. A McCallum, K Nigam. AAAI-98 workshop on learning for text categorization 752, 41-48., 1998.: 2576
4. *Andrew McCallum.* Early results for named entity recognition with conditional random fields, feature induction and web-enhanced lexicons. A McCallum, W Li. Proceedings of the seventh conference on Natural language learning at HLT..., 2003.: 704
5. *Andrew McCallum.* Learning hidden Markov model structure for information extraction. K Seymore, A McCallum, R Rosenfeld. AAAI-99 Workshop on Machine Learning for Information Extraction, 37-42., 1999.: 486
6. *C Lee Giles.* Automatic document metadata extraction using support vector machines. H Han, CL Giles, E Manavoglu, H Zha, Z Zhang, E Fox. Digital Libraries, 2003. Proceedings. 2003 Joint Conference on, 37-48., 2003.: 335
7. *Daniel Weld.* Web-scale information extraction in knowitall:(preliminary results). O Etzioni, M Cafarella, D Downey, S Kok, AM Popescu, T Shaked,... Proceedings of the 13th international conference on World Wide Web, 100-110., 2004.: 721
8. *Daniel Weld.* Open information extraction from the web. O Etzioni, M Banko, S Soderland, DS Weld. Communications of the ACM 51 (12), 68-74., 2008.: 315
9. *Daniel Weld.* Unsupervised named-entity extraction from the web: An experimental study. O Etzioni, M Cafarella, D Downey, AM Popescu, T Shaked, S Soderland,... Artificial intelligence 165 (1), 91-134., 2005.: 891

Рис. 4 – Фрагмент бібліографічного списку з посиланнями на PDF-файли публікацій

Висновки

У запропонованій моделі ПрО як онтологічні зв'язки застосовуються зв'язки між областями інтересів окремих вчених. Фактично розглядається компактифікація біграфа «вчений – наукові поняття, його цікавлять».

Слід відзначити принципову відмінність запропонованої моделі від існуючих, що базуються на аналізі текстових корпусів (наприклад, [2]), або безпосередньої участі експертів при виборі конкретних вузлів і зв’язків [1]. Тут експерт-користувач вкладає лише крупинки знань у вигляді невеликих

за обсягом словників тегів і шаблонів. Далі автоматично використовуються знання, закладені самими авторами публікацій, теги відмічені ними як головні. Тобто експертне середовище в цьому випадку істотно розширюється.

Модель застосована для напрямку досліджень «екстрагування понять», але її можна використовувати і для інших наукових областей. Зокрема, вже побудовані подібні мережі для напрямків штучного інтелекту, багатоагентних системи і складних мереж (Complex Networks).

1. *Добров Б.В.* Онтологии и тезаурусы / Добров Б.В., Соловьев В.Д., Лукашевич Н.В., Иванов В.В. // Модели, инструменты, приложения. Бином, 2009. – 173 с.
2. *Ландэ Д.В.* Подход к созданию терминологических онтологий / Ландэ Д.В., Снарский А.А. // Онтология проектирования, 2014. – № 2(12). – С. 83-91.
3. *Чанышев О.Г.* Автоматическое построение терминологической базы знаний / Чанышев О.Г. // Труды 10-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» – RCDL’2008, Дубна, Россия, 2008. – С. 85-92.
4. *Zeinalipour-Yazti D.* Information Retrieval in Peer-to-Peer Networks / Zeinalipour-Yazti D., Kalogeraki V., Gunopulos D // IEEE CiSE Magazine, Special Issue on Web Engineering, 2004. – pp. 1-13.
5. *Kalogeraki V.* A Local Search Mechanism for Peer-to-Peer Networks / Kalogeraki V., Gunopulos D., Zeinalipour-Yazti D. // Proc. of CIKM'02, McLean VA, USA, 2002.
6. *Yang B.* Efficient Search in Peer-to-Peer Networks / Yang B., Garcia-Molina H. // Proc. of ICDCS'02, Vienna, Austria, 2002.
7. *Erdős, P.* On The Evolution of Random Graphs / Erdős, P., Rényi, A. // Magyar Tud. Akad. Mat. Kutató Int. Közl. 5, 1960. – 17-61 pp.
8. *Albert* Statistical mechanics of complex networks / Albert, Réka; Barabási, Albert-László // Reviews of Modern Physics 74, 2002. – 47–97 pp.
9. *Ландэ Д.В.* Моделирование контентных сетей // Проблеми інформатизаціх та управління: Збірник наукових праць: Випуск 1

ДЕЯКІ ПИТАННЯ ДЕРЖАВНОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ЗАРУБІЖНИЙ ДОСВІД

Лук'янчук Р.В.
Інститут законодавства Верховної Ради України

В сучасних умовах у світовому масштабі спостерігається постійна еволюція кібернетичних атак – від простого блокування роботи Інтернету до активних заходів проти промислових та критичних державних об'єктів інформаційної інфраструктури, операційних систем, у тому числі посягання, націлені на національний кібернетичний простір окремих держав. За оцінками світових експертів у сфері кібербезпеки відмічається стійка тенденція до значного зростання в сучасних умовах кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури.

Також об'єктами кібератак дедалі стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону та захист від надзвичайних ситуацій, а також сервери їх офіційних Інтернет - представництв і електронної пошти [1, с.160].

Чисельні посягання на кіберпростір передових країн світу спонукали світову спільноту віднести кібератаки до проблем політичного характеру та політичного виміру, усвідомлюючи необхідність доповнення діючих стратегій національної безпеки питаннями забезпечення саме кібернетичної безпеки.

Саме тому практично усі національні стратегії забезпечення кібербезпеки пов'язують її проблематику саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет). Широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів. Це пояснюється значним коефіцієнтом «корисної» дії цих загроз, тому що обсяг ресурсів, що витрачаються на реалізацію загроз, є набагато меншим, ніж результати, що отримуються [2, С.57].

За таких умов кібербезпека залишається важливим елементом побудови концептів національної безпеки, і реагування на цей виклик потребує розробки нових стратегічних рішень з боку держави. Так, з метою недопущення будь-яких зовнішніх посягань на національний сегмент кіберпростору політичним керівництвом більшості країн світу, в рамках державного регулювання, було визначено саме мілітаризацію кібербезпеки, що призвело до створення у переважній більшості країн спеціальних підрозділів - військ спеціальних інформаційних операцій.

Так, за останні роки у Великій Британії значно збільшено кількість підрозділів, задіяних у забезпеченні кібербезпеки, які входять до структури Операційного центру кібернетичної безпеки (UK Cyber Security Operations Centre). В Індійській республіці, з метою посилення захисту національного сегменту кіберпростору, відповідні повноваження були передані від підрозділу у складі Міністерства інформації до сектору безпеки і оборони, а саме до «силових» структур, які опікуються питаннями забезпечення національної безпеки. За даними ФБР, Китай на сьогоднішній день має армію у складі 180 тис. хакерів, які займаються щоденними атаками на кібермережі США. При цьому 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору, ключовим завданням яких є отримання доступу до військових та комерційних секретів США, здійснення інформаційних диверсій та запровадження збоїв у роботі інформаційно-комунікаційних систем урядових та фінансових служб.

В оприлюдненому на початку 2013 року звіті американської фірми «Mandiant» із питань кібербезпеки безапеляційно зазначено, що експерти фірми, проаналізувавши численні випадки спроб зламу електронних систем різних компаній і відомств США, дійшли висновку, що сліди ведуть до Китаю, зокрема до розташованої в одному із районів Шанхаю 12-поверхової будівлі, у якій згідно з американськими даними розміщено китайський військовий спецпідрозділ 61398 [3]. У травні 2014 року в міжнародні ЗМІ через Міністерство юстиції США потрапила інформація, що п'яти китайським військовим хакерам з відділу 61398 пред'явлено звинувачення в імовірному викраданні економічних секретів США [4].

Таким чином, за позицією американської сторони, Китай не тільки використовує кібератаки для крадіжок та обробки інтелектуальної власності, але й заробляє гроші шляхом розробки продукції, заснованої на вкраденій інформації.

Експерти з питань військової безпеки США вважають, що досить часто китайські товари, створені на основі викраденої американської інформації, перепродаються назад у США приблизно вдвічі дешевше, ніж оригінальні американські продукти, що є свідченням того, що наразі система китайського режиму з обробки та реверс-інжинірингу (зворотної розробки) крадених технологій стала набагато масштабнішою і сильнішою. Організації, що відповідають за реверс-інжиніринг, офіційно називаються «Національними китайськими центрами обробки технологій». При цьому саме спеціальні інформаційні війська Народно-визвольній армії Китаю (НВАК) відіграють важливу та особливу роль у викраденні інформації.

24 квітня 2015 року за ініціативи Міністерства оборони в США була проголошена оновлена редакція стратегії національної кібербезпеки [5], у положеннях якої визначено основні засади захисту вітчизняної інформаційно-телекомунікаційної мережі, напрями приватно-державного співробітництва у кіберпросторі, умови проведення спеціальних інформаційних військових операцій з використанням особового складу

оперативної групи з питань кібербезпеки «STRATCOM», яка об'єднує ядерні, космічні та кібервійська. Вперше, у положеннях зазначеного акта задекларовано агресивний характер реагування держави на будь-який випадок настання загрози для національного кіберпростору. У вказаному документі такі країни як Китай, РФ, Іран та КНДР визначені потенційними супротивниками, при цьому КНР було звинувачено у промисловому шпіонажі та чисельних крадіжках інтелектуальної власності США з використанням комп'ютерних мереж.

Надійний захист національного сегменту кіберпростору та домінування у світовому масштабі – стратегічне завдання уряду США, що не виключає проведення військових операцій у кіберпросторі з урахуванням площини національних інтересів. Політичний вектор, закладений в стратегії національної кібербезпеки США 2015 року аргументовано декларує систему кіберзагроз, настання яких провокує необхідність проведення спеціальних інформаційних операцій, спрямованих на упередження та недопущення будь-яких кібератак з боку інших держав. Також проведення потужних кібератак є складовою перспективного плану військових дій США з метою зміцнення власних позицій у світовому кіберпросторі.

У положеннях стратегії протистояння загрозам у сфері кібербезпеки також задекларовано, що у США 90% комп'ютерних мереж являють собою приватні бізнес-мережі, тому захист національного кіберпростору залишається не тільки завданням уряду, але у тому числі й приватних технологічних компаній. Вважається, що практична реалізація положень кіберстратегії дозволить до 2018 року оптимізувати в структурі Міністерства оборони США функціонування 133 підрозділів військ спеціальних інформаційних операцій (кібернетичні війська), загальною чисельністю понад 6 тисяч військовослужбовців, які здатні швидко та оперативно реагувати на будь-які кіберзагрози та кібератаки, незалежно від географії місця знаходження технологічних потужностей супротивника. Через структури «STRATCOM» планується інтегрувати «віртуальну реальність», розробити та впровадити у життя уніфіковану технологічну платформу, що дозволить проводити масштабні кібератаки.

Аналіз положень стратегії національної кібербезпеки США свідчить про наміри її політичного керівництва запровадити «гонку кіберозброєння» та підкреслити своє домінуюче становище у світовому кіберпросторі. За задумом військового командування США, нова стратегія дозволить, у тому числі, забезпечити функціонування дієвої системи захисту інформації у закритих інформаційних системах, а також створити нові інтегровані можливості для підтримки військових операцій у надзвичайних ситуаціях.

Забезпечення кібернетичної безпеки будь-якої країни світу неможливо без визначення пріоритетів державної інформаційної політики. Таким чином, більшість країн світу активно модернізують власні сектори безпеки у відповідності до викликів сучасності, і особливо – зважаючи на потенціал використання мережі Інтернет у військових цілях. Цей процес відбувається

шляхом реформування системи державного управління відповідним сектором безпеки, що передбачає: створення та оптимізацію спеціалізованих підрозділів (військ спеціальних інформаційних операцій) та відповідних управлінських структур; розробку власної кібернетичної зброї; посилення державного контролю за національним сегментом кіберпростору, визначення дієвих заходів у сфері боротьби з кібертероризмом.

Література

1. Мовчан А.В. Кібернетична безпека Україна в умовах глобальної нестабільності / А.В. Мовчан // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. - №1 (34). - С.159- 163.

2. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – 2014. - №2(42). – С. 54- 62.

3. Америка обвиняет Китай в кибернападениях // Военно-промышленный курьер. – 2013. – № 8. – 27 февраля. – С. 3.

4. Ексклюзив: китайські шпигуни обкрадають світ на трильйони доларів [Електронний ресурс]. – Режим доступу: http://www.epochtimes.com.ua/novyny-kytayu/eksklyuzi-kitayski-shpguni-okraayut-svt-n-trilyoni-dolariv-121240.

5. Кібернетична Стратегія США [Електронний ресурс]. – Режим доступу: http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

"КІБЕРАТАКА", ЯК СПОСІБ ВЧИНЕННЯ ЗЛОЧИНІВ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Марiц Д.
НТУУ «КПІ»

Розширення інформаційного простору, так чи інакше, опосередковується впровадженням наннотехнологій, ноу-хау, досягнень науки та техніки, Інтернет ресурсів. Це безумовно впливає на інформаційну конкуренцію, а відтак і на кібернетичну безпеку, як окремих суб'єктів у суспільстві так і держави в цілому. За останнє десятиріччя кібернетична безпека сформувалася у самостійний науковий напрям, що має свою специфіку поставлених задач та методів дослідження [1]. У перекладі з грецької, кібернетика – це мистецтво управління. Однак таке управління, а часто-густо і контроль, використовується поза межами правового поля. Тому, не звичним, а можливо і не зрозумілим, на перший погляд, видається переплетіння суто технічних галузей з гуманітарними. Зокрема, у використанні в праві такого терміну як «кібернетична безпека». Тому, спершу вважаємо за доцільне визначитись що таке «кібернетична безпека».

У червні 2013 року Верховною Радою України був розглянутий законопроект від 04.06.2013 року № 2207а «Про кібернетичну безпеку України». Пройшло ще 2 роки і 19.06.2015 року був поданий до розгляду проект № 2126а у новій редакції «Про основні засади забезпечення кібербезпеки в Україні» [2]. У статті першій пропонується наступне визначення кібернетичної безпеки (кібербезпеки), як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Аналізуючи інші нормативно-правові акти, нажаль приходимо до висновку, що законодавець не визначив ключових понять та термінів у сфері кібернетичної безпеки. На сьогодні простежується тенденція виникнення нових понять і термінів, і відповідно «шкутильгання» правотворчості, яка покликана в даному випадку опосередковувати та регулювати правовідносини в інформаційній сфері..

Активне використання технічних засобів у повсякденному житті, кожного із нас, дає ймовірність стати жертвою кіберзлочинців. Тому у цих тезах, зробимо спробу висвітлити один із аспектів на що саме має спрямовуватись кібернетична безпека.

Кібернетичні впливи можуть бути спрямовані на будь-які об'єкти кібернетичного простору, включаючи соціум, соціотехнічні системи, технічні системи у вигляді інформаційних, психологічних та різноманітних фізичних деструктивних впливів [3].

Термін «кіберзлочинність» часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Поняття «кіберзлочинність» (в англомовному варіанті - cybercrime) ширше, ніж «комп`ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Так, Оксфордський тлумачний словник визначає приставку «cyber - » як компонент складного слова. Її значення - що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення міститься у Кембриджському словнику. Таким чином, «cybercrime» - це злочинність, пов`язана як з використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному відноситься до злочинів, скоюваних проти комп`ютерів або комп`ютерних даних [4]. У зв'язку з ратифікацією Україною Конвенції «Про кіберзлочинність» 7 вересня 2005 року вважаємо за доцільне використовувати термін «кіберзлочинність».

Держава Україна останнім часом перебуває у фокусі кібератак. На початку жовтня 2014 року в Києві відбувся П'ятий український Форум з управління Інтернетом (IGF-UA). У рамках форуму IGF експерти провели аналіз кібератак за перші 9 місяців 2014 року. Стан захищеності українського кіберпростору різко погіршився упродовж останніх двох років. У 2014 році Україна посіла 5 місце в рейтингу країн, на які здійснюються кібератаки. Однак, за даними американської компанії, станом на 17 квітня 2015 року Україна і США очолили список жертв шпигунських кібератак. Компанія щорічно проводить дослідження, використовуючи дані міжнародних партнерів у сфері комунікацій, а також дані секретної служби США і департаменту національної безпеки США. Гліб Пахаренко, фахівець з кібербезпеки і захисту даних, зазначив, що аналіз таких подій як Євромайдан, окупація Криму, війна РФ проти України показав, що найважливішими невирішеними проблемами в сфері кібербезпеки є незахищеність критичної інфраструктури, причому не тільки кібератак, а й фізичних атак. Також відзначено високу кількість заражених вірусами і неправильно сконфігурованих систем в українському сегменті Інтернету. Хакерська група «КіберБеркут» – інтернет-бренд, під яким відбуваються хакерські атаки в основному на сайти державних і громадських організацій України. Хто керує брендом невідомо.

Американський спеціаліст з комп'ютерної безпеки Джефрі Карр вважає, що це група проросійських хактивістів. Група офіційно оголосила свої цілі: боротьба з неофашизмом, націоналізмом и свавіллям влади в Україні. «КіберБеркут» має власний сайт і представлений в соціальних медіа. Саме

«КіберБеркут» взяв на себе відповідальність за порушення роботи системи електронного підрахунку голосів на парламентських виборах. Українські ІТ-фахівці спільно з американськими експертами виявили ряд комп'ютерних вірусів, які здійснюють кібератаки на державні органи України, так принаймі заявляє екс-глава «Майкрософт Україна», Дмитро Шимків. Такі віруси, створені російськими спецслужбами спеціально для атак на українські держсайти. Такої думки притримуються американські фахівці. Віруси дуже розумні, грамотно побудовані з інженерної точки зору [5].

Інша група під назвою «КіберОборона», навпаки, захищає українські сайти та електронні реєстри від кібератак – таких, як розпочата в день виборів президента України атака на сервери Центрвиборчкому України, яка, за даними української влади, була здійснена з території Росії. Як повідомляє активіст «КіберОборони» Сергій Костюков, завдання організації захистити кіберпростір України. Великою мірою процес ускладнюється через те, що знову ж таки нема згаданої вище налагодженої співпраці з державою. Активіст наголошує: «Ми розбили нашу ініціативу на кілька етапів, і в міру наростання нашої ініціативної групи ми плануємо десь із кінця літа – початку вересня почати більш систематичні контакти у формі круглих столів, конференцій, різних брифінгів, у тому числі з представниками органів влади, щоб привернути до проблеми більшу увагу. Тому що держава в якомусь сенсі беззахисна перед кібернетичними загрозами» [6].

Усі прогресивні держави світу по-різному намагаються захистити свій віртуальний простір. Тим більш якщо це стосується національної безпеки. Вашингтон готовий санкціями захищати свій віртуальний простір. У Білому домі розглядають можливість замороження активів іноземних осіб і компаній, яких підозрюють у хакерських атаках. Ця інформація, з посиланням на джерела в американській владі, з'явилася одразу в кількох провідних західних виданнях. За їхніми даними, під санкції можуть потрапити представники Китаю та Росії, яких найчастіше звинувачують у незаконному проникненні в систему кібербезпеки американських компаній та відомств. Рішення щодо цих обмежень США мають ухвалити впродовж найближчих двох тижнів.

Тому видається, що в першу чергу необхідно розв'язати такі основні проблеми:

- подолати бар'єр між розвитком нових технологій та правовим полем, шляхом прийняття відповідних нормативно-правових актів;
- посилити міжнародне співробітництво у сфері розслідування кіберзлочинів;
- гармонізувати кримінальне законодавство на міжнародному рівні.

Література

1. http://is.ipt.kpi.ua/kibernetichna-bezpeka-matematichni-metodi-kibernetichnoyi-bezpeki-novi-spetsializatsiyi-fti . - [Електронний ресурс]. – Назва з екрана.

2. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55657/ - [Електронний ресурс]. – Назва з екрана.

3. Даник Ю.Г. Основні аспекти парадигми кібернетичної безпеки. / Ю.Г. Даник. / Науковий вісник Інституту міжнародних відносин НАУ. Серія : економіка, право, політологія, туризм. – 2011. - № 3. – Т. 1 - С. 44-45.

4. Кіберзлочинність: проблеми боротьби і прогнози // http://anticyber.com.ua/article_detail.php?id=140 . - [Електронний ресурс]. – Назва з екрана.

5. http://scienceukraine.in.ua/sciblogs/ukraina-v-fokusi-kiberatak. - [Електронний ресурс]. – Назва з екрана.

6. Там само.

7. США заморожуватимуть активи Росії та Китаю за кіберзлочини // http://podrobnosti.ua/2055686-ssha-zamorozhuvatimut-aktivi-ros-ta-kitaju-za-kberzlochini.html. - [Електронний ресурс]. – Назва з екрана.

АНАЛІТИКА КІБЕРБЕЗПЕКИ: ПОНЯТТЯ, СТРУКТУРА, ЗАДАЧІ

Мохор В.В.[1], Максименко Є.В.[1], Дорогий Я.Ю.[1], Цуркан В.В.[2],
[1]ІСЗЗІ НТУУ «КПІ», [2] ФПМ НТУУ «КПІ»

Головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає кіберпростір. Це обумовлено тим, що сучасні інформаційні технології дають змогу їм реалізувати власні інтереси без застосування військової сили, а також впливати на кібербезпеку конкурентної держави. Тому своєчасне прийняття обґрунтованих рішень про обробляння ризиків за результатами аналітичної діяльності дозволить забезпечити збереження властивостей інформаційних активів в кіберпросторі [1].

Аналітика кібербезпеки тлумачиться як цілісна сукупність принципів методологічного, організаційного та технічного забезпечення індивідуальної та колективної розумової діяльності. Означена діяльність направлена на ефективне опрацювання інформації про вразливості, загрози, ризики безпеці інформаційних активів у кіберпросторі з метою створення інформаційної бази для оцінювання означених ризиків та, як наслідок, прийняття обґрунтованих рішень про їх обробляння [1 – 3].

Структура аналітики кібербезпеки визначається взаємопов’язаними методологічним, технологічним та організаційним напрямками. Внаслідок цього формулюються три класи завдань [2, 3]:

- методологічні;
- технологічні;
- організаційні.

Такий підхід дозволяє, по-перше, визначати актуальні вразливості, загрози та ризики безпеці інформаційних активів у кіберпросторі; по-друге, використовувати методологічне підґрунтя аналітики для створення інформаційної бази про них; як, наслідок, по-третє, забезпечувати інформаційно-аналітичну підтримку прийняття рішень про обробляння актуальних ризиків безпеки інформаційних активів у кіберпросторі.

Література

1. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В. В. Мохор, А. М. Богданов, А. С. Килевой. К.: ООО «Три-К», 2013. – 129 с.

2. Курносов Ю.В. Аналитика : методология, технология и организация информационно-аналитической работы / Ю.В. Курносов, П.Ю. Конотопов. – М. : РУСАКИ, 2004. – 512 с.

3. Паклин Н.Б. Бизнес-аналитика: от данных к знаниям / Н.Б. Паклин, В.И. Орешков. – СПб. : Питер, 2013. – 706 с.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ АДМІНІСТРАТИВНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЙ

Нашинець-Наумова А.Ю.
Київський університет імені Б. Грінченка

Усе більш очевидною стає залежність загального рівня економічної безпеки корпорацій від інформаційної складової. Практика показує, що будь-яка недружня акція, спрямована проти інтересів корпорацій, починається зі збору інформації. Навіть дрібне розкрадання звичайно випереджає вивчення особою зі злочинними задумами можливості протиправних дій і без відповідного інформаційного забезпечення не представляються такі деструктивні прояви, як відведення активів корпорації або рейдерське захоплення. Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі [1, с.70-76].

Інформаційна безпека корпорації – це захист інформації, якою володіє корпорація від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміють захищеність інформації та її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації її власникам або її інфраструктури [2].

Сучасні умови конкуренції та ведення підприємницької діяльності в країні потребують комплексного підходу до вивчення адміністративно-правових методів забезпечення інформаційної безпеки корпорацій, основою яких є адміністративно-правові.

Насамперед метою застосування адміністративно-запобіжних заходів є відвернення або зменшення шкідливих наслідків, які можуть настати внаслідок надзвичайних обставин та/або інших причин, не пов’язаних з вчиненням правопорушення. Завдяки цьому відмежування адміністративно-запобіжних заходів від інших заходів адміністративного примусу, на нашу думку, може відображатися через відсутність зв’язку з неправомірною поведінкою учасника. З точки зору вивчення нашої проблематики, Національна комісія з цінних паперів та фондового ринку (НКЦПФР) має право звертатися до суду з позовом (заявою) про припинення діяльності корпорації внаслідок:

- допущення при її створенні порушень, які неможливо усунути;
- неподання корпорацією НКЦПФР протягом двох років поспіль інформації, передбаченої Законом України «Про державне регулювання ринку цінних паперів».

До примусових заходів ми можемо віднести частину 2 ст. 38 Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців», яка визначає підстави для винесення судового рішення щодо припинення юридичної особи, що не пов'язане з банкрутством юридичної особи. Наступний вид примусового заходу трактується відповідно до ч. 10 ст. 17 та ч. 3 ст. 23 Закону України «Про цінні папери». Торговці цінними паперами та фондові біржі зобов'язані подавати до загальнодоступної інформаційної бази даних НКЦПФР інформацію про всі вчинені за їхньої участі правочини щодо емісійних цінних паперів:

- найменування емітента цінних паперів та його ідентифікаційний код згідно з ЄДРПОУ;
- вид, тип, клас, форму існування та форму випуску цінних паперів;
- міжнародний ідентифікаційний номер цінних паперів;
- кількість цінних паперів за кожним правочином;
- ціну цінних паперів;
- дату вчинення правочину;
- інші відомості, визначені НКЦПФР.

До зазначеної інформації не включаються відомості про сторони правочинів. Порядок та строки подання торговцем цінними паперами зазначеної інформації, а також порядок її подальшого розміщення встановлюються НКЦПФР. Відповідно до ч. 5 ст. 27 Закону України «Про цінні папери» юридична особа, яка є професійним учасником фондового ринку, зобов'язана повідомляти НКЦПФР про всі зміни структури її власності, а також подавати інформацію про ділову репутацію новопризначених керівників у місячний строк із дня настання відповідних змін в установленому Комісією порядку.

Фізична особа, яка є професійним учасником фондового ринку, зобов'язана повідомляти НКЦПФР про всі зміни у відомостях про своїх асоційованих осіб, а також подавати інформацію про свою ділову репутацію в порядку та у строк, які установлені Комісією.

Адміністративно-запобіжні заходи мають превентивний характер, тобто запобігають вчиненню нових правопорушень. Проте, для заходів припинення, попередження правопорушення не є основною, а переважно додатковою ознакою. Також, не всі заходи адміністративного припинення однаковою мірою сприяють запобіганню правопорушенням.

Так, заходи адміністративного припинення застосовуються, зокрема, Національною комісією з цінних паперів та фондового ринку і спрямовані на: припинення порушень правових норм (об'єктивно протиправних діянь); створення умов для подальшого притягнення винних до відповідальності; усунення шкідливих наслідків правопорушення; запобігання вчиненню нових правопорушень; відновлення попереднього, правомірного стану.

Адміністративно-забезпечувальні заходи дозволяють забезпечити: а) виконання рішення про накладання стягнення на порушника; б) провадження справ про правопорушення як в самій корпорації, так і на

всьому ринку цінних паперів; в) формування доказової бази для притягнення порушників до відповідальності.

Таким ознакам відповідають такі примусові заходи: НКЦПФР може зупинити дію ліцензії професучасника фондового ринку на підставі рішення «Про затвердження Змін до Порядку зупинення дії та анулювання ліцензії на окремі види професійної діяльності на фондовому ринку». Прийнятий документ також уточнює причини, за якими НКЦПФР може зупинити дію ліцензії на строк, встановлений таким рішенням.

Зазначене може відбутись у разі:

- проведення перевірки щодо ознак маніпулювання на фондовій біржі;
- незаконного поширення інсайдерської інформації та її використання у власних корисних цілях або корисних цілях інших осіб;
- наявності правопорушення на ринку цінних паперів, за яким триває перевірка і яке може призвести до нехтування правами інвесторів.

Раніше ніж перейти до розгляду наступного методу забезпечення інформаційної безпеки корпорацій – адміністративної відповідальності – нами було з'ясовано, що серед теоретичних розробок, які присвячені цій проблемі визначається повна одностайність думок науковців.

Так, на думку авторів підручника з академічного курсу адміністративного права України, адміністративна відповідальність – це різновид юридичної відповідальності, що являє собою сукупність адміністративних правовідносин, які виникають у зв'язку із застосуванням уповноваженими органами (посадовими особами) до осіб, що вчинили адміністративний проступок, передбачених нормами адміністративного права особливих санкцій – адміністративних стягнень [3, с. 430].

В.К.Колпаков стверджує, що адміністративна відповідальність – це специфічне реагування держави на адміністративне правопорушення, що полягає в застосуванні уповноваженим органом або посадовою особою передбаченого законом стягнення до суб'єкта правопорушення [4, с. 89].

С.Т.Гончарук визначає адміністративну відповідальність як різновид юридичної відповідальності, що передбачає застосування адміністративних стягнень до осіб, які вчинили адміністративні проступки [5, с. 61].

На думку Ю.П.Битяка під адміністративною відповідальністю слід розуміти накладення на правопорушників загальнообов'язкових правил, які діють у державному управлінні, адміністративних стягнень, що тягнуть за собою для цих осіб обтяжливі наслідки матеріального чи морального характеру [6, с. 140].

Найбільш повним, на нашу думку, буде визначення зроблене Д.Н.Бахрахом, на основі наступних ознак, які зазначають що адміністративна відповідальність: а) застосовується за правопорушення, встановлені законодавчими актами про адміністративну відповідальність; б) застосовується широким колом органів адміністративної юрисдикції та

інших, уповноважених законом; в) реалізується в адміністративному провадженні, що має власні процесуальні особливості; г) являє собою реалізацію адміністративних стягнень по відношенню до частково (функціонально) підлеглих суб'єктів; д) може застосовуватись до колективних та індивідуальних суб'єктів [7, с. 126].

Таким чином зрозуміло, що до третьої групи адміністративно-правових методів найчастіше включають лише адміністративні стягнення.

Адміністративне законодавство України передбачає санкції за порушення встановлених правил у сфері забезпечення інформаційної безпеки корпорацій. Вони передбачають такі заходи відповідальності:

- накладання стягнень на юридичних осіб за порушення нормативно-правових положень;
- застосування заходів адміністративного впливу по відношенню до юридичних осіб за порушення нормативно-правових положень.

Суб'єктами скоєння адміністративного правопорушення в сфері забезпечення інформаційної безпеки корпорацій можуть бути: акціонери, посадові особи органів акціонерного товариства, засновники, учасники корпорацій тощо. Перераховані суб'єкти є відмінними за статусом, для кожного з них може бути встановлено різну ступінь вини із врахуванням соціально-економічного чинника відповідного суб'єкта адміністративного правопорушення.

Література

1. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві / Ю. Коваленко // Національна безпека та оборона. – 2001. – № 1. – С. 70-76.

2. Проблема інформаційної безпеки // Спосіб доступу: URL http://ua.textreferat.com/referat-7941-6.html – Загол. з екрана.

3. Козлов Ю.М. Административное право: учебник / Ю.М. Козлов, Л.Л. Попов. – М.: Юрист, 2000. – 567 с.

4. Колпаков В.К., Гордеєв В.В. Докази і доказування в адміністративному судочинстві: Монографія. – Чернівці: Чернів. нац. ун-т. – 2009. – 128 с.

5. Гончарук С.Т. Адміністративний процес: навчальний посібник / Степан Тихонович Гончарук. – К.: НАУ, 2010. – 190 с.

6. Адміністративне право України: підручник / [Битяк Ю.П., Гаращук В.М., Дьяченко О.В. та ін.]; за ред. Ю.П. Битяка. – К.: Юрінком Інтер, 2006. – 544 с.

7. Бахрах Д.Н. Административное право России: учебник / Бахрах Д.Н., Хазанов С.Д., Демин А.В. – М.: Норма-Инфра-М, 2002. – 620 с.

ЗАСТОСУВАННЯ МЕТОДІВ ТЕОРІЇ СКЛАДНИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ТА СТРУКТУРНОГО АНАЛІЗУ КРИМІНАЛЬНИХ МЕРЕЖ

Нечаєв О.О.
Інститут спеціального зв'язку і захисту інформації НТУУ «КПІ»

На даний час використання багатьох засобів комунікацій таких як інтернет та мобільний зв'язок на стільки увійшло в побут кожної людини, що без цього переважній більшості людей важко себе уявити. Окрім того, не менш ніж в побуті, засоби комунікацій використовуються для координації та вчинення злочинних дій. Відомо, що всі перелічені засоби зв'язку залишають гетерогенні сліди в інформаційному просторі та, у встановленим законом порядку, акумулюються правоохоронними органами. В даній роботі представлена теоретична основа для виявлення і класифікації злочинних організацій в мережах створених на основі даних про їх телефонні контакти.

Як правило, кримінальні організації мають чітку структуру, яку в більшості випадків можливо сміливо назвати ієрархічною. В організованому злочинному угрупуванні завжди є лідер та наближені до нього; прості виконавці; ті, що виконують специфічні функції, найбільш цікаві з яких це зв'язки з іншими групами. Також, відомо, що різні ОЗУ контактують між собою.

Кожна особа є окремою індивідуальністю, вона має унікальні відбитки пальців, унікальну обличчя та унікальну поведінку. Проте всі люди мають однакову структуру тіла та природою заложені схожі реакції на зовнішні збуджувачі. Те ж саме можливо сказати і про спілкування людини. Кожна особа має своє унікальне розподілення контактів. Проте їх робочі контакти, близькі соціальні контакти, родинні зв'язки, тощо будуть мати своє у більшості випадків загальні для всіх показники. В мережі контактів членів злочинного угрупування всі по різному будуть спілкуватись з особами, які стоять на вищих ступенях ієрархії, та з тими, що з ними рівні. Також, при великому складі угрупування завжди виділяються внутрішні субструктури, які виконують схожу роботу та входять якщо можливо сказати до одних підрозділів.

Мета роботи

Метою даної роботи є створення теоретичної основи для виявлення і класифікації злочинних організацій в мережах створених на основі даних про їх телефонні контакти. Також, в ході роботи, необхідно сформувати прототипекспертної системи, виявлення в мережах телефонного зв'язку кримінальних мереж та їх субструктур.

Таким чином, виявлення злочинних організацій включає два формалізовані етапи:

1. Викриття таких спільнот у великих телекомунікаційних мережах, можливо на основі достовірно відомої інформації щодо причетності окремих осіб до ОЗУ, або на основі припущення про причетність основаної на статистичному аналізі гетерогенних медіа даних.

2. Другий етап включає вивчення відносин, що існують між членами злочинних угрупувань, динаміка їх зв'язку та ієрархічних відносин, винайдення повної структури організації та ролі кожного її функціонера.

В сучасному світі ці ідеї широко використовуються на комерційній основі, та багато розвинутих країн є їхніми споживачами, але, природно, більшість з реальних досліджень в цій галузі підпадають під гриф державної або комерційної таємниці.

Серед найбільш відомих засобів аналізу візуалізації кримінальних мереж, деякі з яких мають діючі контракти з правоохоронними органами окремих країн світу, можна назвати наступні: COPLINK, Analyst'sNotebook, XanalysisLink Explorer та відомий PalantirGovernment[9].

Виклад основних результатів

Початкові дослідження в області аналізу соціальних мереж (якими фактично є і кримінальні мережі) в 60-х роках в роботахМільграмом і Траверсом [1], де аналізуються характеристики реальних складних мереж, проводяться соціальні експерименти в реальному світі, та представлена так звана «модель малого світу». Згідно даної моделі доводяться докази, що, не зважаючи на велику розмірність, складні мережі показують ряд загальних властивостей: ступеневий розподіл сформованого соціального графа підкоряється степеневому закону, хоча і асимптотично, тобто відношеннявузлів графу, що мають k звязків між собою, до числа усіх першин для великих значень k визначається як: $P(k) \sim k^{-\gamma}$, де γ – це константа, значення якої знаходиться зазвичай у межах $2 < \gamma < 3$, однак інколи значення γ може бути поза цими межами. Також в таких мережах існує відносно короткий шлях, що з'єднує довільну пару вузлів.

А.Барабаши [2] довів модель зростання мережі, яка була декілька разів успішно використана на WorldWideWeb, телекомунакаційних мереж, тощо. Автор довів, що реальні складні мережі мають одну і ту ж динаміку зростання, так звану пільгову прихильність: нові вузли, як правило більше підключаються до вузлів з великим ступенем, ніж до вузлів з нижчим. Ці твердження спричинили виникнення поняття «безмасштабності» мережі (тобто специфічного розподілу вузлів та їх відповідного розвитку), дозволяючи наявність вузлів-концентраторів (вузлів-зірок) та посередників (тих, через які проходить максимальна кількість мінімальних шляхів між довільними парами вузлів). Таким чином «ефект малого світу», привілейована модель зростання, та степеневий розподіл ступенів характеризують структуру соціальної мережі [5].

Основні роботи із застосування аналізу складних мереж для дослідження саме злочинних організацій, їх вразливостей, а також в сфері розвідки належать МалколмуСпарроу[3]. Саме він визначив чотири риси, властиві кримінальним мережам:

1) Обмежений розмір. Кримінальні мережі переважно складаються не більше ніж з 1-2 тисяч вузлів.

2) Неповнота інформації. Кримінальні мережі неминуче містять порожні фрагменти інформації та помилкову інформацію.

3) Невизначені кордони. Важко визначити всі відносини окремих вузлів

4) Динаміка. Нові стійкі з'єднання здійснюються лише з вузлами схожих мережевих структур.

Завдяки М.Спарроу інші автори теж взялись за дослідження кримінальних мереж. На приклад, Бейкер і Фаулкнер[5] вивчали злочинні мережі, зрівнюючи їх розвиток із законами, притаманним електричному обладнанню. Арквілла і Ронфельд[4] узагальнили попереднє дослідження шляхом введення концепції мережевого протистояння тероризму. Останні явно демонструють різницю між звичайними соціальними мережами та кримінальними.

Однак, всі останні роботи нехтують важливістю візуалізації, більш зосереджуючи увагу на статистичних характеристиках мереж, або винайдення параметрів, які б допомогли ідентифікувати роль кожного вузла в мережі.

Лише у 2006 році Валдіс Кребс застосував мережевий аналіз з візуалізацією, який розкрив структуру Аль-Каїди, викритої шляхом аналізу складної мережі створеної на основі телефонних контактів осіб, які мали місце в подіях 11 вересня 2001 року в США [8].

Слід зазначити, що саме після цих подій перед світом найбільш гостро встало питання необхідності розвитку теорії складних мереж для забезпечення державної безпеки. Це створило так би мовити відправну точку серії наукових робіт, в яких аналіз соціальних мереж застосовується на реальних випадках, на відміну від попередніх робіт, використовувавших для дослідів штучні та змодельовані мережі. Тоді, американським урядом було здійснено звернення до вчених та дослідників які можуть надати допомогу у виявленні терористичних груп з метою їх попереднього захоплення та уникнення можливості терористичних актів. Як було відомо із медіа, подальше усунення цієї організації було здійснено саме завдяки методам теорії складних мереж.

Роботи В.Кребса є одним з найбільших відкритих прикладів застосування теорії складних мереж для викриття кримінальних структур.

Зазначені факти доводять ефективність таких технологій та роль, яку вони грають в діяльності сучасних правоохоронних органів. Проте, лише крихти з реальних досліджень не підпадають під гриф або державної або комерційної таємниці.

Аналіз соціальних мереж

Таким чином в кримінології та боротьбі з тероризмом аналіз соціальних мереж (далі SNA – socialnetworkanalysis) став потужним інструментом для викриття структур кримінальних організацій. Він дозволяє зрозуміти позиції кожного вузла в соціальній мережі та особливості взаємозв'язків між вузлами, а також належності окремих вузлів до субструктур. SNA визначає ключові поняття для опису структури мережі та ролей вузлів в ній, основні з яких:

1) Центральність. Відноситься до групи метрик, метою яких є визначення значущості» або «впливу» певного вузла (або групи вузлів) в мережі. Прикладами загальних методів виміру центральності є визначення центральності з посередництва, по близькості, центральності власного вектора, альфа-центральності і центральності за ступенем [15].

2) Міст. Вузол, слабкі зв'язки якого заповнюють структурні прогалини, забезпечуючи єдине з'єднання між двома індивідами (або кластерами, субграфами). Він так само включає в себе найкоротший шлях, коли більш довгий шлях неможливий через високий ризик спотворення повідомлення або неможливості доставки.

3) Закритість мережі. Відображає міру повноти реляційних тріад. Присвоєння вузлам ступеня закритості (тобто того факту, що їх зв'язки в свою чергу зв'язані між собою) називається транзитивністю.

4) Щільність. Ставлення прямих зв'язків в мережі до загального можливій кількості зв'язків. Щільним графом називається граф , в якому число зв'язків близько до максимального . Граф з протилежною властивістю , що має мале число зв'язків, називається розрідженим графом.

5) Посередництво. Відображає кількісне значення, що дорівнює кількості мінімальних шляхів між двома довільними вузлами, які проходять через вузол, що розглядається. Також може розраховуватись значення посередництва між двома зв'язками.

Також, SNAвключає методи виявлення кластерів (або субграфів), визначаючи їх ролі та ролі окремих вузлів в субструктурах, які забезпечуються різними методами графічного відображення мереж. Одні з методів явно призначені для виявлення груп всередині мережі, в той час інші розроблені для виявлення соціальних ролей членів групи. Найбільш поширені методи візуалізації мають матричне представлення та так зване представлення «вузол-зв'язок».

Питання якісної візуалізації, яка б демонструвала всі вище перелічені властивості соціальних мереж набуває все більшого значення. Розвиток візуалізаційних засобів стикається з такими основними аспектами:

1) Вибір алгоритму візуалізації.

2) Представлення динамічної зміни структури графа в часі.

3) Режими запровадження ітеративності для зменшення візуальної складності.

На даний час існує багато засобів візуалізації графів, які мають ті чи інші недоліки та переваги, однак це питання досі є надактуальним. В даній роботі будуть розглянуті найбільш актуальні методи для візуалізації саме кримінальних мереж.

Центральний вузол злочинної мережі може грати ключову роль виступаючи в якості лідера, віддавати накази, забезпечує та контролює інформаційний потік до всіх компонентів злочинної мережі. Видалення таких вузлів може ефективно вплинути на структуру мережі в деяких випадка до припинення нею протиправної діяльності.

Крім того, при аналізі кримінальних мереж слід звернути увагу на підгрупи (або банди), кожні з яких найчастіше грають свою специфічну роль. Взаємодія субструктур між собою дозволяє функціонувати всій злочинній організації як окремому організму. Виходячи з цього, при видаленні окремих вузлів, які зв'язують між собою групи можливо також вчинити великий деструктивний вплив на всю мережу в цілому.

Важливим аспектом аналізу злочинних мереж є забезпечення поповнення аналітичної системи різноплановою інформацією із різних джерел, що надаватимуть якісні структуровані початкові дані для подальшої аналітичної роботи.

Мобільні телефони та різноманітні Інтернет-засоби спілкування постійно використовуються для координації та здійснення протиправної діяльності.

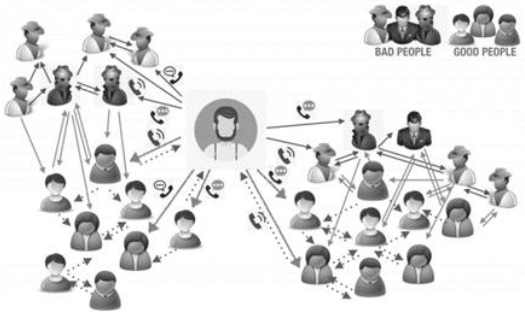


Рис. 1. Телефонні дзвінки

На рис. 1 засобом візуалізації відображені зв'язки підозрюваного. Завдяки відображенню всієї схеми контактів можливо зробити аргументоване припущення, що підозрюваний грає роль посередника між двома субструктурами злочинної організації [5].

Алгоритми візуалізації

Найбільш типовий алгоритм візуалізації графів FDA (force-directedalgorithm) відображає структуру графа як фізичної системи, в якій на

позицію вузла (його координати) впливають різні псевдофізичні сили, та система моделює положення вузлів при якій всі ці сили перебувають в стані найбільшої рівноваги. Цей алгоритм зручно використовувати, коли необхідно продемонструвати об'єднані групи вузлів або кластерів відповідно до рівня зєднаності один з одним. Метод BHA(Barnes-Hutalgorithm) симулює гравітаційну модель в сенсі постійного оновлення позицій вузлів.

Для настройки візуалізації в залежності від тої чи іншої задачіможливоітеративно змінювати параметри відношень між вузлами. В даному випадку можна уявити, що вузли з'єднані між собою пружинами однакової напруженості, що координує позиції відображення вузлів. Ітеративна зміна параметрів являє собою зміну напруженості пружин. Відповідно, вузли з невеликим ступенем (кількістю зв'язків) будуть розташовані в периферійній області, а вузли-хаби в центральній.

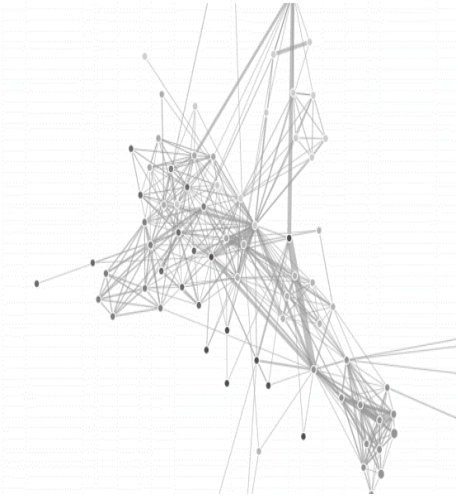


Рис. 2. Приклад force-directed algorithm на невеликій мережі з 75 вузлів

Надалі будуть приведені методи візуалізації специфічного налаштування властивостей FDA для відображення саме злочинних мереж.

Фокус та контекст-орієнтована візуалізація

Кількість зв'язків в мережі іноді швидше росте ніж кількість вузлів. Як наслідок, схема мережі може стати не читаємою через надлишкову щільність зв'язків. Вказана проблема відома як «візуальне перезавантаження». Одним із способів уникнення візуального

перезавантаження є використання функції масштабування тієї частини графа, яка становить найбільший інтерес. Але цей метод має основний недолік – глобальна структура мережі при масштабуванні окремої її частини залишається без уваги. Поміж тим, така методика захисту від надлишковості може бути застосована в злочинних мережах через їх, як сказано вище, по-перше квазіієрархічну структуру, та по-друге в порівнянні з іншими мережами помірний розмір.

Також, у правоохоронних органів регулярно виникає необхідність перевірити зв'язки конкретної людини (підозрюваного), та такий вид візуалізації демонструє високі показники при візуалізації невеликих мереж. Основна задача аналізу мережі в більшості випадків полягає в виявленні нечітких (або латентних) зв'язків розглядаємої особи з кримінальними або іншими колами. Тому, в даному випадку, слід зосереджуватися на окремих контактах, а не всій мережі в цілому і її структурі.

В класичному варіанті FDA не передбачає застосування методики фокусування на окремій часині графа. Але, наявні спеціальні модифікації цього алгоритму, які дозволяють це робити: «риб'яче око» (Fisheye FDA) та «фокус» (Foci FDA) [12-13].

Модифікація Fisheye FDA

Даний алгоритм так би мовити, відображає фокус в залежності від контексту.

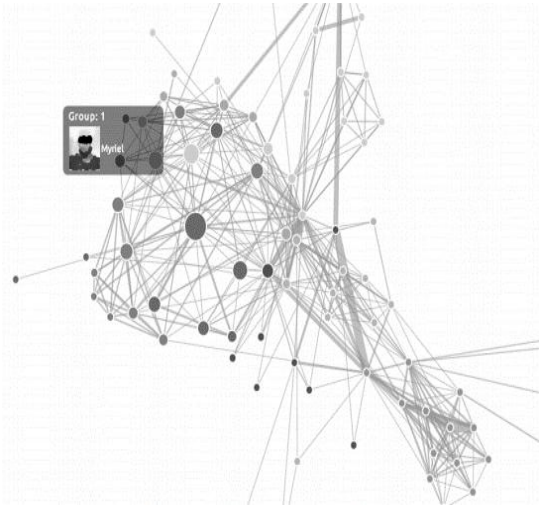


Рис. 2. Приклад Fisheye FDA, на тій же мережі

Даний алгоритм дозволяє користувачу зосередитись на одній або декількох областях соціального графа та динамічно настроювати фокус. Вперше даний алгоритм був запропонований для візуалізації самоорганізаційних карт Кохонена (Self-organizing map — SOM) В. Фурнасом [10]. Цей метод відомий тим, що вносить певне якісне спотворення класичної візуалізації. Це метод розширення, який дозволяє не збільшуючи розмір самого простору відображення значно розширити область навколо фокусу та стиснути райони віддалені від фокусу, при цьому зберігаючи загальну структуру мережі.

Модифікація Foci FDA.

Даний тип візуалізації об'єднує FDA, семантичний та кластерний методи відображення. Він оснований на алгоритмі виявлення субструктурЛовіана. Даний алгоритм підтримує багаторівневий аналіз з плаваючим гравітаційним центром.

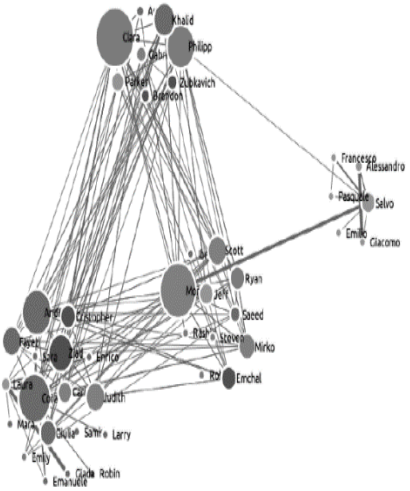


Рис. 3. Приклад Foci FDA, на тій же мережі

Даний метод візуалізації дозволяє об'єднує щільно зв'язані субграфи в один вузол, що демонструє непогані показники при необхідності зображення повної структури всієї злочинної мережі. В той же час, можливо розкрити окрему субструктуру та детально аналізувати відношення між членами конкретної групи.

На рис. 3 продемонстрована кластеризація, що в даному випадку відображає територіальний поділ між групами, які належать одній організації.

Візуалізація мереж з використаннямгео-маппінгу

Також необхідно торкнутись методів візуалізації з прив'язкою до територію. Оскільки відомо, що всі телефонні контакти здійснюються через базові станції мобільного зв'язку, на які зберігаються координати. Також, кожна базова станція має декілька секторів в радіусі своєї дії та запам'ятовує радіус (або направлення) з якого абонент здійснює телефонний або інший контакт, який визначає кут охоплення сектору антени. Ці дані не дозволяють точно локалізувати місцезнаходження абонента на момент зв'язку, тим не менш можливо приблизно локалізувати користувачів, що потрапляють в конкретну зону дії базової станції.

Рис. 4. Приклад візуалізації з з використанням гео-маппінгу

Використання даного типу відображення кримінальних мереж надає унікальні аналітичні можливості зі спостереження місцезнаходження членів ОЗУ або підозрюваних у певний момент часу (наприклад під час вчинення злочину). Необхідно вказати, що дана методика візуалізації може не тільки скоротити час аналітичної обробки великих масивів інформації та представити її в зручному вигляді, але, у багатьох випадках зробити такий аналіз загалом можливим.

Висновки

Протягом останніх 10-12 років спостерігається активне залучення вчених та дослідників для вивчення злочинних та терористичних мереж з метою виконання задач із забезпечення громадської та державної безпеки розвинутих країн світу. В даному аспекті, аналіз соціальних мереж надає гнучкі та ефективні інструменти для виявлення злочинних мереж на основі їх цифрових слідів в інформаційному просторі, що активно розвивається; виявлення структури злочинних організацій та розбиття їх на підгрупи, які, як правило, зосереджені на виконанні тих чи інших задач; встановлення взаємозв'язків між окремими функціонерами ОЗУ, а також між окремими бандами та групами; вивчення інформаційних потоків в кримінальному середовищі; та виявлення тих функціонерів таких груп або зв'язків між окремими з них, при яких злочинна мережа може припинити свою протиправну діяльність або зовсім перестати існувати.

З урахуванням викладеного, дослідження теорії складних мереж в контексті забезпечення державної та громадської безпеки набуває все більшої актуальності та необхідності запровадження її методів в повсякденній роботі правоохоронних.

Література

1. Travers, Jeffrey & Stanley Milgram. 1969. "An Experimental Study of the Small World Problem." Sociometry, Vol. 32, No. 4, pp. 425-443.
2. A.-L. Barabási, A.Réka, "Emergence of scaling in random networks", Science, 286:509-512, October 15, 1999.
3. M. K. Sparrow. The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13(3):251–274, 1991.
4. J. Arquilla and D. Ronfeldt. Networks and netwars: The future of terror, crime, and militancy. Survival, 44(2):175–176, 2001.
5. W. Baker and R. Faulkner. The social organization of conspiracy: illegal networks in the heavy electrical equipment industry. Am. Social. Rev., 58, 1993.
6. E. Ferrara, P. De Meo, S. Catanese, and G. Fiumara. Detecting criminal organizations in mobile phone networks. Expert Systems with Applications, 41(13):5733–5750, 2014.
7. P. Klerks and E. Smeets. The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators.Connections, 24:53–65, 2001.
8. V. Krebs. Mapping networks of terrorist cells. Connections, 24(3):43–52, 2002.
9. C. Morselli. Assessing vulnerable and strategic positions in a criminal network. JournalofContemporaryCriminalJustice, 26(4):382–392, 2010.
10. F. Schneider, A. Feldmann, B. Krishnamurthy, and W. Willinger. Understanding online social network Internet conference, pages 35–48. ACM, 2009.
11. H. Zang, F. Baccelli, and J. Bolot. Bayesian inference for localization in cellular networks. In 2010 Proceedings IEEE INFOCOM, pages 1–9. IEEE, 2010.

12. J. Xu and H. Chen. Criminal network analysis and visualization. Comm. ACM, 48(6):100–107, 2005.
13. C. Yang, H. Chen, and K. Hong. Visualization of large category map for internet browsing. Decis. SupportSyst., 35(1):89–102, Apr. 2003.
14. C. Yang, N. Liu, and M. Sageman. Analyzing the terrorist social networks with visualization tools. InIntelligence&securityinformatics. 2006.
15. L. Freeman. A set of measures of centrality based on betweenness. Sociometry, pages 35–41, 1977.

БІЖЕНЦІ З БЛИЗЬКОГО СХОДУ, ЯК ЗАГРОЗА ХРИСТІАНСЬКІЙ ІДЕНТИЧНОСТІ ЄВРОПИ

Петряєв О.С.
Національний інститут стратегічних досліджень при Президентові України

Нагальні події, які відбуваються в Європі протягом поточного 2015 року, різко змінили усталені геополітичні акценти розвитку всього суспільства. Під подіями маємо на увазі безкомпромісну атаку Старого Світу з боку нелегальних мігрантів з країн Близького Сходу й Північної Африки. Про те, як була спровокована ця ситуація, які об'єктивні причини, інформаційні і організаційні технології спрацювали каталізаторами цієї події, а також перспективи ісламізації Європи, ми спробуємо зазначити в даному тезисі.

Масова міграція народів Близького Сходу та Північної Африки в країни Європейського Союзу (ЄС), стала однією з значущих подій року, яке залишиться в історії цивілізації. В деякій мірі,цю подію можна порівняти з початком великого переселення народів світу, що відбувалося в Європі уIV-VII століттях. Причинами міграції стали тривалі війни в Лівії, Сирії, Іраку та Ємені,і нестабільна політико-економічна ситуація в Лівані, Єгипті та Тунісі. Частка відповідальності за розв'язування громадянських війн, що тривають вже багато років,лежить на Європейських державах, які безпосередньо брали участь у військових операціях протизаконних урядів зазначених країн,активно підтримуючи їх опозиційні сили.

Руйнування в цих країнах державних інститутів та інфраструктури, збідніння,та наступ хаусу, призвели до створення на даних територіях нового територіального утворення з ознаками державності та терористичним режимом під назвою «Ісламська держава» (ІД). Тривалість і жорстокість, з якою відбуваються військові зіткнення, призвели до гуманітарної катастрофи і поставили на межу виживання цивільне населення цих країн.Дана ситуація закономірно породила безвихідне положення корінного населення, яке було змушене покинути свої домівки.

Перша хвиля біженців відбула спрямована на сусідні країні – Йорданію, Ліван та Туреччину, де у продовж років сконцентрувались сотні тисяч біженців. Крім того, одночасно розпочалися невеличкі спроби нелегальної міграції до країн ЄС, де відпрацьовувалась система організації міграції та канали нелегального переходу кордонів.

Однією з мотивацій спрямування потоків біженців до ЄС стала широко розповсюджена інформація про високий рівень життя в цих країнах, терпимість їх населення до інших культур, релігій, та політика мультикультуралізму. Крім зазначених арабських країн, в Європу потяглися мігранти, що сповідують іслам з Конго, Малі, Еритреї, Пакистану, Афганістану тощо, які не є арабами. В той же час, мігранти, не зажадали переселятися в країни монархії Перської затоки, так як там існує жорстке

міграційне законодавство, строгі релігійні правила і зневажливе ставлення до вихідців з арабських країн Північної Африки та Леванту.

Хоча громадянські війни на зазначених територіях тривають вже багато років (від року до десяти в залежності від країни), масова міграція до країн Західної Європи почалась лише у поточному році, коли ЄС погруз у банкрутстві Греції, та економічному ослабленні більшості країн її членів, що поставило питання про можливий початок її розпаду. Крім того, значним тягарем стала втрата російського ринку в умовах приєднання ЄС до економічної блокади Росії.

Не важко було помітити, що друга хвиля біженців до країн ЄС принципово відрізняється від першого своєю **швидкістю, масовістю та організованістю.** За таких умов лідери та населення ЄС не були готові до прийняття такого виклику. Принцип мультикультуралізму, як головне досягнення Європейського Союзу, став суттєвим гальмовим фактором в організації зупинення нелегальної міграції. Більш того, цей принцип був врахований організаторами даної акції. Додатково, з метою переформатування свідомості мешканців країн ЄС, збудження співчуття до незаконних мігрантів, через засоби масової інформації був запущений сюжет про загибель трьох річного хлопчика, який разом зі своїми батьками тікали з охопленої вогнем Сирії [1]. З даного приводу треба зауважити, що до цього сюжету мешканців Європи не бентежила загибель тисяч біженців на шляху до «європейської мрії».

За перше півріччя 2015 року в ЄС прибуло 340 тис. нелегальних біженців, що на 170 відсотків більше аналогічного періоду минулого року. Серпень і вересень стали апогеєм, і можуть перевищити вже зафіксовані цифри, адже щоденно до узбереж Греції та Італії прибувають від чотирьох до десяти тисяч біженців[1]. За заявою міністерства закордонних справ Угорщини «*у бік Європи направляється 30-35 мільйонів біженців*»[2].

У цьому контексті важливо звернути увагу, що поряд з нелегальними мігрантами, безумовно є бойовики ісламісти з Ісламської держави, емісари вербувальники та ісламські проповідники. За неперевіреними даними служб безпеки ЕС численність ісламських бойовиків може скластидо 4 тисяч [3].Безумовно, що дана категорія нелегалів становить загрозу, не тільки для безпеки Європейських громадян, а й для християнської цивілізації в тому числі. Ісламські проповідники, ведуть проповіді, проповідуючи радикальне течії в ісламі, салафізм та ваххабізм. Небезпека цього вчення в ісламі, полягає в його не терпимості до інших релігій, і агресивне нав'язування ісламу, не правовірним мусульманам.

Безумовно, що зростання населення ЄС завдяки арабським та іншим біженцям ісламського віросповідання рано чи пізно приведе до їх протистояння до європейської культури та християнської віри. Адже історична пам'ять завжди залишається у народів світу і передається від покоління до покоління. Навіть проте, що уряди країн ЄС будуть намагатися інтегрувати мусульманських біженців до культури і правилам життя в своїх

країнах, все одно протистояння неминуче і, випадково або штучно,спалахне обов'язково.

Такою ситуацією обов'язково скористаються ісламські емісари проповідники, які несуть радикальний іслам, і направляють мусульманське населення Європи на боротьбу (джихад) проти європейських християн. В деякій мірі, дане судження можна підкріпити фактом згоди уряду Саудівської Аравії на фінансування будівництва мережі мечетей для біженців у розрахунку однієї на кожні сто мусульман, про що свідчить одна з провідних німецьких газет "Frankfurter Allgemeine Zeitung", посилаючись на Ліванську газету AlDiyar (Аль-Діяр)[4].

Судячи із заяв уряду Саудівської Аравії, можна зробити висновок, що Арабське королівство зацікавлене не тільки в арабізації Європи, але і її ісламізації, що може призвести до етнічних, політичних і релігійних конфліктів у Європі.

В свою чергу, прем'єр міністр Угорщини Віктор Орбан зазначив, що справжня мета мусульманських біженців не є порятунок від бойових дій в країнах з яких вони тікають, а дістатися до багатих європейських країн, таких як Німеччина, Австрія та Швеція. Крім того, він висловив стурбованість, майбутнім європейської цивілізації, з масовим приходом мусульманського
населення, яке в осяжному майбутньому може становити загрозу для Європи [5].

Сформована ситуація в Європі, була описана американським політологом Самуеля Гантінгтономв роботі "Зіткнення цивілізацій" у 1993 році.Зтеоретичної точки зору, автор розглянув майбутні конфлікти, які мажуть виникнути на основі загальних принципів цивілізації через релігію, мову, культуру і традиції. Не дивлячись на те, що конфлікти які ґрунтуютьсяна економічних і політичних розбіжностях не зникнуть, до них додадуться конфлікти на релігійному ґрунті, і розбіжності культур. У той же час, країни які мають спільну релігію, мову і культуру, будуть об'єднуватися для протидії іншим ворожим цивілізаціям [6].

Якщо провести історичну паралель з подіями періоду великого переселення народів, про яке згадувалося на початку тези, то не важко помітити навала переселенців того періоду до південних територій Європи, де був високий рівень життя у порівнянні з північними землями Європи. У кінцевому рахунку, ця міграція стимулювала падіння Західної Римської імперії.

Література

1. Миграционный кризис в ЕС: Кто, куда и откуда? [Електронний ресурс]. – Режим доступу: http://informing.ru/2015/09/08/migracionnyy-krizis-v-es-kto-kuda-i-otkuda.html

2. МИД Венгрии: в сторону Европынаправляется 30-35 миллионовбеженцев.[Електронний ресурс]. – Режим доступу: http://ria.ru/world/20150918/1260210092.html

3. Islamic-State-ISIS-Smuggler-THOUSANDS-Extremists-into-Europe-Refugees. [Електронний ресурс]. – Режим доступу: http://www.express.co.uk/news/world/555434/

4. Al. Withnall- SaudiArabiaoffersGermany 200 mosques – oneforevery 100 refugeeswhoarrivedlastweekend. [Електронний ресурс]. – Режим доступу: http://www.independent.co.uk/news/world/europe/saudi-arabia-offers-germany-200-mosques-one-for-every-100-refugees-who-arrived-last-weekend-10495082.html

5. Refugees threaten Europe's Christian roots, says Hungary's PM. [Електронний ресурс]. – Режим доступу: http://www.jpost.com/Christian-News/Refugees-threaten-Europes-Christian-roots-says-Hungarys-PM-415070

6. Хантингтон С.Ф. Столкновение цивилизаций? [Електронний ресурс]. – Режим доступу: http://gtmarket.ru/laboratory/expertize/2007/2498

К ВОПРОСУ О ПРИРОДЕ И ПОНЯТИИ ИНФОРМАЦИИ

Петряев С. Ю.
ФСП НТУУ «КПИ»

В последние десятилетия мир столкнулся с новым вызовом общественных отношений, в основу которых легли информационные технологии. Информационная составляющая общества формирует не только перспективное его развитие, но и обнажает множество проблем, нуждающихся в правовом, административном и социальном регулировании. Это, прежде всего, влияние информационных технологий на безопасность общества, государства и человека в частности. Без четкого понимания природы информации, сути этого явления, сложно формулировать дефиниции.

На тему о значении информации, ее влияния на развитие и социализацию общества, написано масса научных трудов. Не меньше сделано попыток ответить на давно волнующий всех вопрос о природе информации, как явления бытия. Опровергая друг друга, ученый истеблишмент, по сути, разделился на два лагеря, отстаивая разными доводами свои позиции и опровергая чужие, которые, так или иначе, сводятся к идеальному или материальному объяснению природы информации.

Среди ученых бытует сентенция, если выбросить из философии даже самую маразматическую теорию, она сразу обеднеет. Поэтому мы позволим себе порассуждать о понятии такого природного явления, как информация, ибо «даже самая негативная определенность положительна хотя бы тем, что расставляет точки над «i», делает ситуацию более ясной и понятной. В данном случае можно каким-либо образом спрогнозировать будущее развитие событий и построить в соответствии с данным прогнозом практическую деятельность. Самое худшее из всего возможного - неопределенность, парализующая любую деятельность, лишающая нас любых ориентиров» [1].

Не претендуя на серьезность и оригинальность суждений, ниже мы приведем наше представление на данное явление, тем более, что общепринятого научного понятия информации, которое бы удовлетворяло всех ученых, пока нам не довелось встретить, а желание откопать философский камень, не дает покоя.

Информация как мед заполняет соты нашего сознания, формируя осмысленную картину окружающих событий, и объясняет суть бытия. Если следовать за устойчивой мыслью о том, что информация – есть суть человеческого мышления (воспринимается, формируется, хранится, передается и уничтожается) то, что же тогда есть связи, протекающие в условиях бытия и формирующие эту информацию, и которые человек пытается познать через свои органы чувств (зрение, слух, обоняние,

осязание и определение вкуса)? Сегодня мы даже знаем, как у человека протекает процесс формирования информации (через биофизические и биохимические процессы), создавая, тем самым, знания об окружающем мире.

Всякое событие (как явление) – это движение, даже если оно кажется нам статичным, так как статика относительна, а значит абстрактна. Мир существует и развивается только благодаря движению – движению частиц разных энергий, образующие систему связей микро и макромиров. Это суть рождения, существования, смерти и вновь рождения материи, то есть жизни бытия. Так существует вселенная, о чем, по крайней мере, нас упорно пытаются убедить астрофизики. Последние их теоретические расчеты в исследовании черных дыр космоса показали, что информация о поглощаемом объекте отражается от края чёрной дыры, словно мячик отскакивает от стены или луч света — от зеркала [2]. Кроме того, область компьютерных технологий пополнилась новыми разработками хранения и передачи информации на основе не электронов (с чем мы имеем дело сегодня), а фотонов света, тем самым, в несколько раз увеличив память процессоров и скорость обработки информации [3].

Эти исследования подтверждают, что только движение различных форм энергий формирует (или возбуждает) информацию, которая передается от одного явления к другому, от одной материи другой, включая человека, который с позиции своего биологического, психического и физического естества, представляет всего узкий диапазон приемника и источника этих энергий (иногда ее называют тонкой материей). И вполне очевидно, что основными законами и принципами движения частиц разных энергий выступают – закон сохранения энергии, отражение материального мира, поглощение и его преобразование (изменение).

Чем же отличается человек от любой другой материи во вселенной, рассматривая себя чуть ли не единственной субстанцией, способной воспринимать, обрабатывать, передавать и хранить информацию? Да ничем, он точно такая же материальная субстанция, существующая по тем же физическим законам движения материи и лишь иронией обстоятельств нашей солнечной системы, природа сформировала нас такими, какими мы есть – мыслящими, способными к анализу информации.

Другими словами, человек выступает субъектом информации, способным принимать, передавать и преобразовывать энергетические потоки точно так же, как любая материя вселенной. Нам просто повезло и мы забываем, что являемся маленькой частицей другого, значительно большего мира.

Наше мышление, есть ни что иное как, движение энергии (электричества) по сосудам нервной системы к нейронам головного мозга, который выступает в роли мощного биологического процессора. Нейтроны, избирательно, получив электрический сигнал, выделяют различные химические молекулы, формирующие соответствующую реакцию на

физические (включая эмоциональные и мыслительные) действия. Таким образом, получаемая человеком информация формируется электрической энергией в виде системы импульсов нейронов мозга. Это подобно компьютерному процессору, на котором записана матрица в виде набора бит, формирующих сложные программные продукты, способные решать различные задачи. Это подобно вселенной, в которой благодаря потокам различных форм энергий, материальный мир избирательно (по случайным или закономерным связям) связан между собой, как нейтроны человеческого мозга, воспринимая или пропуская, преобразуя или отдавая, уничтожая или сохраняя (накапливая) энергоинформацию. Без этих связей нет движения, а нет движения, нет информации, а значит, нет жизни.

Сегодня мы уже можем констатировать, что тенденции развития научной мысли свидетельствует о перспективе создания человеком искусственного интеллекта. Зачатки тому уже существуют, пусть примитивные, но научно-техническая мысль подводит нас к этому решению, что еще раз подсказывает, что информация материальна.

Другими словами, информация – это жизнь бытия, его материально-энергетическое дыхание, способ его существования (включая человека) благодаря потокам различных форм энергий. Развивая данную мысль, мы даже можем предположить, что информационное (виртуальное) пространство, которое сформировало для себя современное человечество – тоже материально. А учитывая то, что информация обладает еще и всеми универсальными свойствами, выступает не только коммуникатором общественных отношений, но и всего бытия.

Из этого следует, что информация есть объективная субстанция бытия (движение различных форм энергий), которая существует в единстве с пространством, материей и временем, определяется ими, проявляется во всех формах бытия, обладает универсальными свойствами и выступает его коммуникатором.

Данный подход к пониманию природы информации не есть новым, но с позиции последних научных открытий в области астрофизики, физики и информатики, на наш взгляд, более приемлемый.

Литература

1. Д.А. Гусев - Философия как наука История и теория классического скептицизма. [Электронный ресурс] – Режим доступа:
http://www.psyoffice.ru/8/filosofy/book_o018_page_8.html

2. Чёрные дыры могут зеркально отражать информацию. [Электронный ресурс] – Режим доступа: http://www.vesti.ru/doc.html?id=2664328.

3. Новая оптическая память может произвести революцию в компьютерных вычислениях. [Электронный ресурс] – Режим доступа: http://www.vesti.ru/doc.html?id=2667554#

ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ: ЯК ЗАБЕЗПЕЧИТИ ЩОБ НЕ НАШКОДИТИ?

Поперечнюк В.М.
НДІІП НАПрН України

Інформаційні суспільні відносини, бодай, чи не одні із найскладніших суспільних відносин, що підлягають правовому врегулюванню. Їх динамічний та активний розвиток, іноді ставить законодавця у глухий кут, а відсутність системної упорядкованості законодавчих актів у цій сфері, на рівні кодифікованого акту, породжує колізії та плутанину в інформаційному законодавстві, що лише поглиблює і без того наявні проблеми.

На сьогоднішній день, однією з найбільших проблем правової системи України є відсутність реалізації превентивної функції права, що законодавчо передбаченими механізмами дозволяє попередити негативні події та явища соціального характеру.

Можливо, сьогодні ми не мали б стільки свідчень на користь якісно проведених інформаційно-психологічних операцій та не констатували б факт інформаційної агресії з боку РФ і неспроможності й безсилля як і влади, так і суспільства адекватно протистояти цьому. «Звичка» реагувати на наявні, а не потенційні загрози цього разу виявилась пагубною для української держави та її населення. Статистика втрат серед військового та мирного населення просто приголомшує, не лишаючи часу на роздуми, оцінки та аналіз, адже цей час для України минув.

Сьогодні нагальним питанням для української влади є забезпечення національної безпеки та інформаційної, як її складової. Проте забезпечення інформаційної безпеки людини, суспільства та держави має здійснюватись таким чином, щоб не нашкодити іншим життєвоважливим інтересам, у першу чергу людини.

На часі гостро стоїть питання контентного наповнення інформаційних ресурсів, зокрема щодо дотримання усіх гуманістичних засад та основних принципів інформаційних суспільних відносин, що передбачені ст. 2 Закону України «Про інформацію» [1]. Головним джерелом одержання інформації є ЗМІ (у т.ч. Інтернет та телебачення), що поширюють її «зі швидкістю звуку», є простими та доступними у своєму використанні, а головне – вимагають від людини мінімум зусиль.

На жаль, на думку автора, забезпечити прозорість та неупередженість діяльності ЗМІ (навіть за наявності політичної волі у суб’єктів владних повноважень) дуже тяжко, адже одразу ж почнуться закиди щодо порушення Конституції України, у т.ч. її норм що закріплюють: свободу

думи і слова, заборону цензури тощо. Головне що вони дійсно будуть обґрунтованими.

Діючи норми вітчизняного законодавства, не в силі не те що захистити чи, як мінімум, убезпечити людину від негативного (деструктивного) впливу інформації, а навіть, постфактум, притягнути винних осіб до відповідальності. «Хитра» норма Закону України «Про інформацію»: «Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень. – далі законодавець пояснює, що ж мається на увазі. – Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.» [1] – коментар зайвий.

Хоча Закон України «Про основи національної безпеки України» до загроз національним інтересам та національній безпеці в інформаційній сфері відносить: «Намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [2]. Тобто, недостовірну та/або упереджену інформацію цілком можна подати, як оціночні судження, тим самим безкарно створювати загрози національним інтересам та національній безпеці України. Взагалі, цілком поділяючи думку Фурашева В.М., що під «оціночні судження» можна вміло завуалювати безліч відомостей та даних що завдають деструктивного (м'яко кажучи), а іноді відверто шкідливого, впливу суспільним відносинам [3, с. 102].

Для справедливості варто зазначити, що той таки Закон України «Про основи національної безпеки України», у тій же ст.7 загрозою також вважає: «Прояви обмеження свободи слова та доступу до публічної інформації» [2]. Отже, поки покладатися на законодавця у питаннях правового забезпечення інформаційної безпеки марно.

У якості висновку, автор не пропонує панацею, а лише хоче зауважити, що ефективною є не лише пряма, а й асиметрична відповідь супернику чи то опоненту. Як говорить народна мудрість: «Поінформований – значить озброєний» – тобто наша «зброя» це знання та інформація (об'єктива та конструктивна), яку людина може використовувати і як щит, і як меч. Єдине, що потрібно українській нації вміти аналізувати, піддавати критиці та верифікації отриману інформацію й ефективно її використовувати, а для цього треба навчитись думати.

Література

1. Про інформацію: Закон України від 02.10.92 р. // Відомості Верховної Ради України. – 1992 р. - № 48. – Ст.650. : в редакції Закону України від 13.01.11р. № 2938-VI // Відомості Верховної Ради України. – 2011. – № 32. – С. 313.

2. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19.06.2003 №964-IV – Режим доступу: http://zakon1.rada.gov.ua/laws/show/964-15

3. Фурашев В.М. Дилема прав і свобод людини в інформаційній сфері в контексті забезпечення інформаційної безпеки // Філософські та суспільно-правові проблеми становлення і розвитку інформаційного суспільства: Матеріали круглого столу / 20 березня 2013 р., м. Київ / Упорядн.: Андрусишин Б. І., Майстренко І. А., Пилипчук В. Г., Фурашев В. М. – Ужгород. – ТОВ "ІВА". – 2013. – С. 100-104.

СЦЕНАРІЇ ПРОТИДІЇ ДЕСТРУКТИВНИМ ВПЛИВАМ НА КОМП'ЮТЕРНІ ІНФОРМАЦІЙНІ МЕРЕЖІ ДЛЯ ВИСОКОТЕХНОЛОГІЧНИХ ОБ'ЄКТІВ

Путятин В.Г., Куценко С.А.
Институт проблем реєстрації інформації НАН України

1 Актуальність проблеми

Протидія деструктивним впливам на комп'ютерні інформаційні мережі для високотехнологічних об'єктів (КІМ ВТО) - це «безперервний процес нагляду за динамічним середовищем, в якому щодня з'являються нові загрози»[1]. Протистояти можливості деструктивних впливів можна тільки завдяки організації та дотриманню певної визначеної політики протидії, яка включає комплекс заходів, что можна об'єднати загальним сценарієм - сценарієм протидії деструктивним впливам на КІМ ВТО.

Поняття *сценарію протидії деструктивним впливам* тісно пов'язане з поняттям *сценарію деструктивного впливу*. Якщо сценарій деструктивного впливу на КІМ ВТО можна визначити, як комплекс дій, что проводяться з метою порушення стійкості функціонування КІМ ВТО, то сценарій *протидії* деструктивним впливам можна визначити, як сукупність взаємопов'язаних процедур прогнозування сценаріїв деструктивного впливу та класифікації комп'ютерних атак порушника, аналізу вразливих місць і технологічних циклів управління КІМ, застосування методів і моделей протидії атакам та оцінки стійкості функціонування КІМ в умовах деструктивних впливів.

Необхідність розробки такого сценарію і визначення порядку дієвих заходів пояснюється розширенням спектру загроз безпеці КІМ ВТО. Цей процес обумовлений зростаючим рівнем інформатизації суспільства, яка не тільки прискорює розвиток цивілізації, а й породжує нові загрози національної, регіональної та глобальної безпеки.

При модернізації та розвитку КІМ на основі застосування нових інформаційних технологій виникає проблема, яка полягає в тому, що мережева архітектура КІМ і цифрове комунікаційне обладнання, необхідні для підвищення надійності інформаційно-обчислювального процесу та оперативності передачі даних, є джерелом і нових уразливостей в разі дії деструктивних впливів взагалі і кібератак зокрема. Поняття *уразливості* можна визначити як властивість комп'ютерної системи, наявність якої може дозволити зловмиснику завдати шкоди системі, інакше кажучи, призвести до реалізації загрози інформаційній безпеці. Тому, для забезпечення стійкості функціонування КІМ при виконанні регламентів збору, доставки та обробки інформації необхідно забезпечити вимоги з протидії деструктивним впливам та розробити чіткий порядок її дотримання

Визначимо основні характерні риси сучасних деструктивних впливів на КІМ: кількісне зростання; масштабність і висока технологічність їх

виконання; висока потенційна небезпека наслідків таких акцій, пов'язаних із значною кількістю жертв, зниженням рівня обороноздатності і безпеки держави, руйнуванням небезпечних виробництв тощо; прийняття у свої арсенали нових засобів і методів інформаційного впливу, зокрема «хакерських» методів, використання різних прихованих каналів [2] (пам'яті або часу), в тому числі і в першу чергу, в глобальному інформаційному просторі (кіберпросторі); професіоналізм і підготовленість джерел деструктивних впливів (кіберзлочинців, кібертерористів, державних структур, супроводжуючих і здійснюючих інформаційні деструктивні операції); постійно зростаюча технічна оснащеність терористичних угруповань і злочинних співтовариств.

Як відомо, деструктивні інформаційні впливи можуть бути спрямовані на досягнення наступних цілей: порушення конфіденційності - розкриття інформації особами, що не мають права доступу до неї; порушення цілісності - несанкціонована модифікація; порушення доступності - недоступність ресурсу (інформації, сервісу, пристрою).

Умови деструктивних впливів на КІМ полягають в реалізації таких подій: 1. Введення помилкових вхідних даних; 2. Порушення інформаційної взаємодії між абонентами КІМ; 3. Відмова у видачі, доставці даних та обміні інформацією; 4. Ініціалізація помилкових подій реконфігурації КІМ; 5. Введення помилкових розрахункових даних; 6. Введення помилкових результатів обробки інформації; 7. Перевантаження абонентів КІМ «спамом» технологічних результатів обробки інформації.

2. Проблема інформаційного вторгнення в КІМ із застосуванням інформаційної зброї

Аналіз сучасного стану проблеми безпеки свідчить про те, що зараз, як ніколи актуальна проблема інформаційного вторгнення в комп'ютерні мережі із застосуванням інформаційної зброї. Вихід цієї загрози на перший план пов'язаний з тим, що сучасні системи управління є системами критичних додатків з високим рівнем комп'ютеризації. Інформатизація нашого суспільства веде до створення єдиного світового інформаційного простору, в межах якого проводиться накопичення, обробка, зберігання та обмін інформацією між суб'єктами цього простору - людьми, організаціями, державами. Інформаційна зброя принципово відрізняється від усіх інших засобів ведення війни тим, що за її допомоги можуть вестися (і вже ведуться) неоголошені і найчастіше невидимі світові війни, і що об'єктами впливу цієї зброї найчастіше є цивільні інститути суспільства і держави: економічні, політичні, соціальні і т.д. Вже визнано, що мережі передачі даних перетворюються на поле битви майбутнього. Інформаційна зброя може використовуватися з «електронними швидкостями» при нападі й обороні.

Інформаційну зброю можна визначити, як засоби знищення, перекручення чи розкрадання інформаційних масивів, засоби подолання

систем захисту, обмеження допуску законних користувачів, дезорганізації роботи апаратури і комп'ютерних систем в цілому. Атакуючою інформаційною зброєю сьогодні можна назвати: 1) комп'ютерні віруси, здатні розмножуватися, проникати в програми, передаватися по лініях зв'язку, мережах передачі даних, виводити з ладу системи управління і т. п.; 2) логічні бомби - запрограмовані пристрої, які встановлюються в інформаційно-керуючі центри військової або цивільної інфраструктури, щоб за сигналом або у встановлений час привести їх у дію; 3) засоби порушення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації у каналах державного та військового управління; 4) засоби нейтралізації тестових програм; 5) помилки різного роду, які свідомо вводяться порушниками в програмне забезпечення об'єкту.

Вважається, що для запобігання або нейтралізації наслідків застосування інформаційної зброї необхідно здійнювати наступні заходи: 1) захист матеріально-технічних об'єктів, що становлять фізичну основу інформаційних ресурсів; 2) забезпечення нормального та безперебійного функціонування баз і банків даних; 3) захист інформації від несанкціонованого доступу, її спотворення чи знищення; 4) збереження якості інформації (своєчасності, точності, повноти і необхідної доступності).

Безпека інформації комп'ютерних мереж досягається проведенням єдиної політики захисних заходів, а також системою заходів правового, організаційного та інженерно-технічного характеру.

Аналіз існуючого стану справ показує, що рівень заходів, що передбачаються для захисту інформації, як правило, нижче рівня автоматизації. Таке відставання може обернутися надзвичайно серйозними наслідками. Засоби протидії повинні відповідати концепції повного і ешелонованого захисту. Це означає, що їх слід розміщувати на концентричних колах, в центрі яких знаходиться об'єкт захисту. У цьому випадку всі можливі шляхи противника до будь-якого об'єкту перетинатимуть ешелоновану систему захисту. Кожен рубіж оборони організовується так, щоб затримати нападника на час, достатній для прийняття персоналом охорони заходів у відповідь. Обрані засоби протидії об'єднують відповідно до прийнятої концепції захисту.

3. Системи виявлення атак

Зростання в останні роки числа наведених проблем, пов'язаних з комп'ютерною безпекою, привело до того, що ключовим компонентом будь-якої стратегії мережевого захисту стали системи виявлення атак (вторгнень) - IDS (Intrusion Detection Systems). За останні кілька років їх популярність значно зросла, оскільки значно покращилася якість і сумісність програм цього напрямку [4].

IDS або детектори атак - це програмні комплекси, побудовані для моніторингу хостів та мереж для повідомлення про небажану активність, або повідомлення та реагування на неї. IDS можуть моніторити активність

певного хосту, групи хостів, або активність мережі, та характеризувати активність, як "підозрілу" чи "аномальну" (тобто таку, що відрізняється від звічайної) шляхом порівняння з набором певних відомих ознак некоректного застосування системи або ознак мережевої атаки.

Механізми, що застосовуються в сучасних системах виявлення атак IDS, засновані на декількох загальних методах, які не є взаємовиключними. У багатьох системах використовуються їх комбінації.

Класифікація IDS може бути виконана: за способом реагування; за способом виявлення атаки; за способом збору інформації про атаку.

За способом реагування розрізняють пасивні та активні IDS.

Пасивні IDS просто фіксують факт атаки, записують дані в файл журналу і видають попередження. Активні IDS намагаються протидіяти атаці, наприклад, шляхом реконфігурації мережевих екранів або генерації списків доступу маршрутизатора.

За способом виявлення атаки системи IDS прийнято ділити на дві категорії: виявлення аномальної поведінки (аномалія на основі); виявлення зловживань (зловживання або виявлення на основі сигнатур).

Технологія виявлення аномальної поведінки заснована на наступному. Аномальна поведінка користувача (атака або яка-небудь ворожа дія) часто проявляється як відхилення від нормальної поведінки. Прикладом аномальної поведінки може служити велике число з'єднань за короткий проміжок часу, високе завантаження центрального процесора і т. п.

Якщо можна було б однозначно описати профіль нормальної поведінки користувача, то будь-яке відхилення від нього можна ідентифікувати як аномальну поведінку. Однак аномальна поведінка не завжди є атакою. Наприклад, одночасне посилання великої кількості запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу «відмова в обслуговуванні».

При використанні системи з такою технологією можливі два «неприємні» випадки: виявлення аномальної поведінки, яка не є атакою, і віднесення її до класу атак; пропуск атаки, яка не підпадає під визначення аномальної поведінки. Цей випадок більш небезпечний, ніж помилкове віднесення аномальної поведінки до класу атак.

Технологія виявлення аномалій орієнтована на виявлення нових типів атак. Однак недолік її - *необхідність постійного навчання*. Поки ця технологія не отримала широкого розповсюдження. Пов'язано це з тим, що вона важко реалізується на практиці.

Виявлення зловживань полягає в описі атаки у вигляді сигнатури (signature) і пошуку даної сигнатури в контрольованому просторі (мережевому трафіку або журналі реєстрації). В якості сигнатури атаки може виступати шаблон дій або рядок символів, що характеризують аномальну діяльність. Ці сигнатури зберігаються в базі даних (БД), аналогічній тій, яка використовується в антивірусних системах. Дана технологія виявлення атак дуже схожа на технологію виявлення вірусів, при

цьому система може виявити всі відомі атаки. Однак системи даного типу не можуть виявляти *нові, ще невідомі види атак.*

Підхід, реалізований у таких системах, досить простий і саме на ньому засновані практично всі пропоновані сьогодні на ринку системи виявлення атак.

Найбільш популярна класифікація *за способом збору інформації про атаку*: виявлення атак на рівні мережі (network-based); виявлення атак на рівні хоста (host-based); виявлення атак на рівні додатку (application-based).

Система *network-based* працює по типу сніффера, «прослуховуючи» трафік у мережі і визначаючи можливі дії зловмисників. Такі системи аналізують мережевий трафік, використовуючи, як правило, сигнатури атак і аналіз «на льоту» - моніторинг мережевого трафіку в реальному або близькому до реального часу і використанні відповідних алгоритмів виявлення.

Системи *host-based* призначені для моніторингу, детектування і реагування на дії зловмисників на певному хості. Розташовуючись на хості, вони перевіряють і виявляють спрямовані проти нього дії. Ці системи аналізують реєстраційні журнали операційної системи або програми.

Як правило, аналіз журналів реєстрації є доповненням до інших методів виявлення атак, зокрема до виявлення атак «на льоту». Використання цього методу дозволяє проводити «розбір польотів» вже після того, як була зафіксована атака, для того, щоб виробити ефективні заходи запобігання аналогічним атакам в майбутньому.

Система *application-based* заснована на пошуку проблем в певному додатку.

Кожен з цих типів систем виявлення атак (на рівні мережі, на рівні хоста і на рівні додатку) має свої переваги і недоліки. Гібридні IDS, що представляють собою комбінацію різних типів систем, як правило, включають в себе можливості декількох категорій.

Комплексний підхід до організації процесу виявлення атак (загроз) представлений в (5). Виходячи з того, що система виявлення атак повинна функціонувати *адекватно* загрозам безпеки, характерним для конкретних об'єктів комп’ютерної інформаційної мережі, акцент пропонується зробити саме на *виявленні та прогнозуванні передумов появи загроз*, властивих для даної КІМ. Перехід від пошуку сигнатур атак до виявлення передумов виникнення загроз інформаційній безпеці КІМ повинен сприяти тому, щоб докорінно змінити ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання.

4. Методи реагування

Атака не тільки повинна бути виявлена, але і необхідно правильно і своєчасно зреагувати на неї. В існуючих системах застосовується широкий спектр методів реагування, які можна розділити на три категорії:

повідомлення; збереження; активне реагування. Застосування тієї чи іншої реакції залежить від багатьох факторів.

Повідомлення. Найпростішим і широко поширеним методом повідомлення є відправлення адміністратору безпеки повідомлень про атаку на консоль системи виявлення атак. Така консоль може бути встановлена не у кожного співробітника, що відповідає в організації за безпеку, крім того, цих співробітників можуть цікавити не всі події безпеки, тому необхідно застосування інших механізмів повідомлення. Цими механізмами можуть бути відправлення повідомлень по електронній пошті, факсом або телефоном. До категорії «повідомлення» відноситься також посилання керуючих послідовностей до інших систем, наприклад до систем мережевого управління або до мережевих екранів.

Збереження. До категорії «збереження» відносяться два варіанти реагування: реєстрація події в БД; відтворення атаки в реальному масштабі часу.

Перший варіант широко поширений і в інших системах захисту. Для реалізації другого варіанту буває необхідно «пропустити» атакуючого в мережу компанії і зафіксувати всі його дії. Це дозволяє адміністратору безпеки потім відтворювати в реальному масштабі часу (або із заданою швидкістю) всі дії, здійснені атакуючим, аналізувати «успішні» атаки і запобігати їм надалі, а також використовувати зібрані дані в процесі розгляду.

Активне реагування. До цієї категорії належать наступні варіанти реагування: блокування роботи атакуючого; завершення сесії з атакуючим вузлом; управління мережевим обладнанням і засобами захисту. IDS можуть запропонувати такі конкретні варіанти реагування: блокування облікового запису атакуючого користувача, автоматичне завершення сесії з атакуючим вузлом, реконфігурація мережевих екранів і маршрутизаторів і т. д. Ця категорія механізмів реагування, з одного боку, досить ефективна, а з іншого боку, вимагає акуратного використання, оскільки неправильне застосування може призвести до порушення працездатності всієї КІМ.

5. Підходи до організації протидії деструктивним впливам на КІМ ВТО

Перш за все, для організації ефективної протидії проявам деструктивних впливів на КІМ ВТО необхідний докладний і всебічний аналіз, систематизація та формальний опис предметної області, включаючи: способи ідентифікації, систематизації та категоризації об'єктів захисту, як елементів тієї чи іншої критичної інфраструктури, що має свої особливості та відповідні загрози; способи визначення рівня захищеності КІМ і методи оцінки ризиків реалізації проти них деструктивних інформаційних впливів; способи (механізми і моделі, засоби і системи) організації протидії проявам кібертерористичних загроз на всіх рівнях комплексного підходу до

забезпечення інформаційної безпеки КІМ: нормативно-правовому; адміністративному; процедурному та організаційно-технічному.

У [6] запропоновано стратегію, що дозволяє здійснювати багаторівневу протидію деструктивним впливам: 1. Попередження атак - визначення потенційних загроз комп'ютерних атак на основі аналітичної інформації та моніторингу. 2. Виявлення атак - виявлення ознак атак в інформації, програмах і в циркулюючих потоках даних. 3. Аналіз атак - розпізнавання і каталогізація комп'ютерних атак відповідно до прийнятої їх класифікації. 4. Активна протидія атакам і забезпечення стійкості функціонування - блокування або нейтралізація деструктивних впливів.

Стосовно до КІМ запропонована стратегія протидії полягає у наступному:

1) у формуванні єдиного простору параметрів протидії комп'ютерним атакам (параметрів стану КІМ і системи захисту (СЗ), ознак атак, параметрів засобів протидії деструктивним впливам (ЗПДВ) і стійкості функціонування КІМ);

2) в урахуванні різнорідних чинників протидії комп'ютерним атакам на КІМ: виявленні (розпізнаванні в структурі параметрів інформаційно-обчислювального процесу) відомих і невідомих атак; необхідності виконання заданого технологічного циклу управління; збереженні стійкості функціонування КІМ в умовах впливу комп'ютерних атак;

3) розробці алгоритму протидії комп'ютерним атакам;

4) розробці причинно-наслідкових математичних співвідношень, що визначають конкретну логіку і обмеження на вирішення проблеми протидії комп'ютерним атакам;

5) розробці шкали показників протидії комп'ютерним атакам;

6) розробці узагальненого методу протидії комп'ютерним атакам на основі теорії розпізнавання образів;

7) реалізації активної протидії атакам і забезпеченні стійкості функціонування КІМ.

6. Сценарій протидії деструктивним впливам на КІМ ВТО

Виходячі із даної стратегії, процес протидії деструктивним впливам на КІМ ВТО повинен відбуватися в декілька основних етапів:

- *підготовчий етап* визначення потенційних загроз, попередження, виявлення та аналізу комп'ютерних атак, який закінчується аналітичним обгрунтуванням характеристик об'єкту захисту і ЗПДВ;

- *етап планування*, який в основному полягає в розробці вимог до складу та функцій ЗПДВ;

- *етап розробки ЗПДВ*, що полягає в тому, що у вузли КІМ впроваджуються датчики і проводиться налагодження мережі об'єкта, що аналізується;

- *етап експериментальної оцінки* дозволяє відпрацювати сценарій застосування ЗПДВ: імітація впливу атак (імітація, доставка, вплив),

протидія атакам (збір інформації від датчиків, виявлення, аналіз, візуалізація, активна протидія).

Управління процесами протидії комп'ютерним атакам реалізується наступним чином: запис даних моніторингу в сервер баз даних моніторингу стану стійкості функціонування і безпеки КІМ; візуалізація результатів роботи керуючих програм датчиків з використанням 2D-моделей (двовимірного представлення даних, як правило, в табличній формі), 3D-моделей (тривимірних моделей комп'ютерної графіки), геоінформаційних систем, на яких наносяться розташування компонентів КІМ і динамічні характеристики виконання технологічного циклу управління та результатів протидії атакам з прив'язкою до електронної карти; аналіз ситуації стосовно впливу атак з порівнянням фактичної інформації про атаки з базами даних сигнатур атак, функціональним аналізом та аналізом аномалій; прийняття в автоматизованому режимі рішень оператором з коригування функцій управління системи захисту, підвищення рівня захищеності і стійкості функціонування КІМ; вибір параметрів протидії комп'ютерним атакам і запуск засобів активної протидії джерелам деструктивних впливів.

З урахуванням вищенаведеного сценарій протидії деструктивним впливам на КІМ ВТО может бути представлений у вигляді наступної послідовності дій:

Попередження атак (виявлення ознак підготовки атаки): сканування вразливостей КІМ ВТО; виявлення ознак пасивного сканування; виявлення ознак активного сканування.

Виявлення атак (збір, реєстрація даних датчиків): моніторинг стійкості функціонування КІМ; попередній аналіз результатів моніторингу;

Аналіз атак (ідентифікація, каталогізація даних про атаки): обробка даних; ідентифікація атаки; корекція еталону технологічного циклу управління КІМ; корекція БД сигнатур.

Протидія атакам (усунення джерел атак): визначення джерела атак; прийняття рішень; вибір заходів і засобів протидії; застосування засобів протидії; оцінка стану стійкості функціонування КІМ; нейтралізація атак; відновлення стійкості функціонування КІМ; візуалізація результатів протидії.

7. Основні принципи попередження деструктивних впливів на КІМ ВТО

В основу політики попередження можливості деструктивних впливів на КІМ ВТО мають бути покладені такі принципи:

Принцип неможливості минати захисні засоби означає, що всі інформаційні потоки в підсистеми КІМ і з них повинні проходити через СЗ.

Надійність будь-якої СЗ визначається *найслабшою ланкою*. Часто такою ланкою виявляється не комп'ютер або програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неприпустимості переходу у відкритий стан означає, що за будь-яких обставин (у тому числі і позаштатних), СЗ або цілком виконує свої функції, або повинна повністю блокувати доступ.

Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо для запобігання зловмисних або некваліфікованих дій системного адміністратора.

Принцип багаторівневого (ешелонованого) захисту наказує не покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні йти програмно-технічні засоби, за ідентифікацією й аутентифікацією - керування доступом і, як останній рубіж, - протоколювання й аудит. Ешелонована оборона здатна, принаймні, затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно заважає непомітному виконанню злочинних дій.

Принцип різноманітності захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗ.

Принцип простоти і керованості системи в цілому і СЗ особливо визначає можливість формального або неформального доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип загальної підтримки заходів безпеки носить нетехнічний характер. Рекомендується з самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на його постійне навчання (теоретичне і, головне, практичне).

Література

1. Ланде Д.В. Безпека в глобальних інформаційних системах та мережах: навчальний посібник / Ланде Д.В., Зубок В.Ю., Мохор В.В. – К.: ІСЗЗІ НТУУ «КПІ», 2010. – 100 с.

2. Гайкович В.Ю. Основы безопасности информационных технологий. / Гайкович В.Ю., Ершов Д.В. – М: МИФИ, 1999. – 96 с.

3. Технологии обнаружения атак [Электронный ресурс] / Your Private Network, апрель 2010г. Режим доступа: http://ypn.ru/448/intrusion-detection-technologies/.

4. Костров Д. Системы обнаружения атак, URL: www.ByteMag.ru

5. А.В. Аграновский. Новый подход к защите информации – системы обнаружения компьютерных угроз [Электронный ресурс] /А.В. Аграновский, Р.А. Хади. Jet Info №4, апрель 2007г. Режим доступа:

http://www.jetinfo.ru/stati/novyj-podkhod-k-zaschite-informatsii-sistemyobnaruzheniya-kompyuternykh

6. Климов С.М. Противодействие компьютерным атакам. Технологические основы: Электронное учебное издание. /Климов С.М., Сычев М.П., Астрахов А.В. - М.: МГТУ имени Н.Э. Баумана, 2013. – 70 с.

ІНФОРМАЦІЙНА БЕЗПЕКА ДИТИНИ, ЯК ЗАПОРУКА НАЦІОНАЛЬНОГО БЛАГОПОЛУЧЧЯ ДЕРЖАВИ

Радзієвська О.Г.
НДІІП НАПрН України

На думку українського дослідника інформаційної політики та комунікаційних технологій Г. Почепцова будь-які суспільні трансформації, перетворення та зміни неможливі без виникнення, усвідомлення та прийняття соціумом нових основоположних змістів та ідей. [1] Ці змісти виникають на основі застарілих рудиментарних ідей внаслідок їх заміщення, або нав'язуються ззовні. Нав'язані ззовні ідей, як правило, є нетиповими для даного соціуму, а тому сприймаються індивідуальною та масовою свідомістю з певним супротивом. Змінити масову свідомість значно легше, чим індивідуальну. Для запуску певних ідей та деякого бажаного змісту в індивідуальну свідомість використовуються методики впливу на індивіда через масову свідомість. Проте як індивідуальна, так і масова свідомість людей чинять певний супротив зовнішньому впливу.

Для якнайшвидшого досягнення поставленої мети та подолання супротиву до прийняття нових змістів, наразі широко застосовуються ЗМІ та Інтернет. Сучасний стан розвитку та використання інформаційно-комунікаційних технологій дозволяє зробити процес впливу на індивідуальну та масову свідомість людини значно ефективнішим, швидшим та всеохоплюючим. Останнє підтверджують соціологічні дослідження. Так, 83,5 % респондентів вважають саме телебачення основним джерелом інформації про події в Україні [2]. Настрої у дитячому середовищі тотожні настроям загалом. Серед основних джерел отримання інформації 38 % українських дітей у віці 7-14 років вважають телебачення, 18 % — комп'ютер (DVD, ігри тощо) і 44 % — Інтернет. На питання про те, яким джерелам для отримання знань вони надають перевагу: телебаченню, Інтернету або інформації, що подається на уроках, учні відповіли таким чином: телебачення — 38 %, Інтернет — 49 %, інформація, отримана на уроках, — 13 % [3].

Дитина, як особа з високим рівнем психічної та психологічної нестабільності, значно легше і швидше піддається інформаційному впливу через масову свідомість. Прикладом цього є колективне навчання у навчально-виховних закладах. Оскільки свідомість дитини не є сталою, з чіткими моральними, етичними та національними цінностями, а знаходиться в процесі інтенсивного формування, то такий потужний інформаційний тиск несе у собі багато ризиків та загроз психічному та моральному здоров'ю дитини, а відтак, і суспільному здоров'ю усієї нації. Свідомість дитини практично не здатна чинити супротив зовнішньому впливу, проте, вона не

потребує й трансформацій, бо є свого роду Tabularasa[3], відкритою до нових ідей, змістів, цінностей, стилів мислення та способів буття. За допомогою інформації ми передаємо дитині знання, формуємо особистість, закладаємо основи її суспільного буття, а відтак, будуємо фундамент наступного покоління та створюємо вектор розвитку як для послідуючих поколінь, так й для суспільства загалом. Тому дуже важливо уже сьогодні замислитись над тим, яка саме інформація запишеться на tabularasa дитячої свідомості і яких саме нових змістів набуде суспільство у майбутньому.

Уже другий рік держава Україна перебуває у стані неоголошеної війни. Сам факт війни завжди вносить певні корективи у кількісний та контекстний склад інформаційних повідомлень, а відтак, значно корегує весь інформаційний простір держави та емоційний стан її громадян. Інформація є предметом нематеріальним. Сприймаючись на свідомому чи підсвідомому рівні, вона чинить безпосередній або опосередкований вплив на духовний світ людини та її емоційний стан. Поняття «інформація» та «емоції людини» тісно пов'язані між собою: будь-яка інформація викликає емоції, емоційний стан безпосередньо впливає на сприйняття інформації та прийняття подальших рішень особистістю. [4] Перенасиченість інформаційного простору інформацією, подекуди недостовірною та суперечливою, ускладнює її аналіз та переосмислення. А все це разом створює чудові умови для маніпулювання свідомістю. Соціальне незадоволення та політична нестабільність стають передумовою того, що екранна агресія та насилля знаходять своє відображення у повсякденному житті на раніше спокійних і мирних територіях.

Що стосується дитячого середовище – то воно, як правило, є дзеркальним відображенням дорослого соціуму. Уже сьогодні сформовані російською пропагандою моделі поведінки переносяться у реальне життя, де відточуються за рахунок ролевих ігор та закарбовуються у свідомість маленьких громадян. [5]

Психіка дитини менш стабільна, а емоційність у сприйняття інформації дитиною значно перевищує емоційність сприйняття дорослого. Дошкільнята та діти молодшого шкільного віку взагалі слабо розрізняють події віртуального та реального світів. Картинка з екрану для них настільки ж реальна як і будь-яка подія із повсякденного життя. [6] Страшні картини наслідків війни їх лякають. Проте, наскільки сильним є вплив того чи

[3]Tabula rasa —латинський вираз який використовується на означення явища що виникає на «пустому місці», не є продовженням якоїсь традиції і формується лише під впливом зовнішніх впливів та власної природи, щооб'єкт в певній сфері не має зв'язків з минулим і може розвиватися в будь-якому напрямку. Термін «табула раса» вживається також щодо дитини як об'єкта виховання, щодо людського розуму, свідомості, душі, яка вміщує у собі враження від зовнішнього світу. [https://uk.wikipedia.org/wiki/Tabula_rasa]

іншого жахіття, залежить від багатьох обставин: віку, емоційного стану дитини, місця перегляду, контенту, і найголовніше – від індивідуального сприйняття побаченого свідомістю окремої дитини. [6, с. 78]

Поміж іншого існує й опосередкований вплив негативної інформації як на свідомому, так і на підсвідомому рівні. Деякі страшні картини війни можуть надовго закарбувати у підсвідомості дитини та у майбутньому стати причиною прихованих страхів (психічних розладів) на довгі роки. [6] Пригнічення емоційно-вольової сфери дитини за рахунок перенасичення інформаційного простору негативною інформацією призводить до її інфантильності, замкнутості, відсутності бажання до навчання та жаги пізнання. А це негативно впливатиме на інтелектуальний та духовний рівень дитини. Замкнутість дитини перешкоджатиме здобуттю комунікативних навичок, що створюватиме складності у спілкуванні та її соціалізації.

Іншим аспектом опосередкованого інформаційного впливу на свідомість дитини є вплив через найближче коло її оточення. Перебуваючи у стані емоційного збудження та агресії, дорослі дуже часто власне незадоволення переносять на самих незахищених членів свого оточення – дітей. Це може бути як у вигляді образ, морального приниження, так і у вигляді фізичного насилля. Таким чином, крім прямого негативного інформаційного впливу від безпосередньої дії повідомлень на дитину, маємо ще й опосередкований вплив через дорослих, що уже стали жертвами інформаційного впливу. Слід також відмітити і той факт, що погляди, думки, звички та й загалом стиль життя дитини формується, перш за все, під безпосереднім впливом найближчого кола спілкування – сім'ї. Як правило, думка одного із батьків (як найбільш авторитетної особи) є для дитини домінуючою і беззаперечно правильною. Таким чином, закладаючи певні інформаційні змісти у свідомість дорослого, ми автоматично здійснюємо непрямий вплив на формування свідомості дитини.

Перенасиченість інформаційного простору різноманітними ідеями, у тому числі і небезпечними, та відсутність єдиної державної політики в інформаційні сфері з системним моніторингом інформаційного простору та адміністративно-правими засобами забезпечення інформаційної безпеки, не тільки викривляє внутрішній світ дітей, але й активно залучає їх у групи, секти та інші об'єднання, діяльність яких може не лише зашкодити інтелектуальному та духовному зростанню, а й становить реальну загрозу їх життю. Все це унеможливить розвиток цілісної високоінтелектуальної та високодуховної особистості зі стійкими життєвими орієнтирами та моральними цінностями, що становитиме у майбутньому основу української нації.

Резюмуючи викладене, хотілось би зазначити, що сучасний інформаційний простір перенасичений різноманітною інформацією, проте не є тим середовищем, в якому безпечно та безперешкодно зростало б майбутнє покоління.

За відсутності критичного мислення та нездатності аналізувати великі об'єми інформації, маніпулювати дитячою свідомістю значно легше чим свідомістю дорослого. Природна довірливість дитини робить її легкою здобиччю для маніпулятора, що, в свою чергу, може призвести до формування у дитини хибних уявлень про загальнонаціональні та загальнолюдські цінності. У світлі прийняття Росією нової військової доктрини [7], беззаперечним є й той факт, що у стані інформаційно-психологічної війни, що веде сьогодні країна–агресор проти нашої держави, свідомість будь-якого громадянина, а особливо дитини, є об'єктом посягань і потребує посиленого захисту.

Враховуючи безсистемність, хаотичність та практично відсутність превентивних заходів протидії негативним інформаційним впливам у державі, наші діти лишаються практично беззахисними. Лише комплексна система організаційних та правових заходів, починаючи від виховання у дитини медіаграмотності та правосвідомості на початкових етапах виховання до нормалізації суспільних відносин у сфері діяльності засобів масової інформації (ЗМІ) у тому числі і Інтернет-ЗМІ, посилення відповідальності за розповсюдження інформації, що не відповідає вимогам законодавства і може призводити до деструктивних наслідків, здатна захищати свідомість дитини на кожному з етапів її дорослішання та сформувати цілісну особистість, як запоруку розвитку та благополуччя нашої держави. Проведення національної інформаційної політики як у державі так і за її межами повинна базуватись на основних правах і свободах громадян та основах інформаційної безпеки, що стає дедалі вагомішою складовою національної безпеки. Необхідно створити концептуальні основи системних заходів убезпечення особистості від негативних інформаційних впливів та плану(послідовності) їх реалізації. Концепція інформаційної безпеки та Національна програма інформаційної безпеки могли б стати основою інформаційної політики у державі на перспективу і дороговказом для вироблення заходів протидії негативним інформаційним впливам на свідомість громадян у різних сферах. Зважаючи на постійно зростаючу загрозу інформаційного впливу й переорієнтацію світу на новий вид протистояння та війни із залученням свідомості та умів молоді, слід консолідувати зусилля психологів, соціологів, політологів, педагогів, правознавців, фахівців з інформаційної безпеки та ін. у створенні Концепції інформаційної безпеки дитини.

Література

1. Почепцов Г. Новыесмыслы, «ломающие» страны. – Електронний ресурс. – Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_smysly_lomayuschie_strany/

2. ЗМІ та довіра до українських і російських ЗМІ. – Електронний ресурс. – Режим доступу: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=425&page=3

3. Іванов В. Ф., Іванова Т. В. Медіакомпетентність та медіаграмотність як основні компетентності сучасного педагога // Інформаційне суспільство. – 2014. – № 20. – С. 96-99.

4. Савінова Н.А. Емоція права: на шляху розуміння наслідків правової комунікації в контексті кримінально-правової комунікації // Інформація і право. – 2015. - № 2(14). – С. 5-12.

5. В Россиидети уже играют в войну с Украиной,— депутат из РФ. - Електронний ресурс. – Режим доступу: http://apostrophe.com.ua/news/politics/2015-05-14/v-rossii-deti-uje-igrayut-v-voynu-s-ukrainoy---deputat-iz-rf/24097

6. Брайант Д., Томпсон С. Основывоздействия СМИ. – М., К., 2004. – 424 с.

7. Военная доктрина РоссийскойФедерации - Електронний ресурс. – Режим доступу: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf

ЩОДО ОСОБЛИВОСТІ ПРОФІЛАКТИКИ ТЕРОРИЗМУ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Рижов І.М.,
НА СБ України

Тероризм відноситься до числа самих небезпечних і важкопрогнозованих явищ сучасності, що набуває все більш різноманітних форм та загрозливих масштабів. Терористичні акти найчастіше приносять масові людські жертви, спричиняють руйнування матеріальних і духовних цінностей, які в майбутньому не піддаються відновленню, сіють ворожнечу між державами, провокують війни, недовіру і ненависть між національними та соціальними групами.

З квітня 2014 року на сході України проводиться широкомасштабна антитерористична операція із залученням сил та засобів багатьох суб'єктів боротьби з тероризмом, з використанням усього арсеналу військових методів і за ознаками фактично являє собою повноцінний локальний збройний конфлікт, обтяжений інформаційно-пропагандистськими маніпулятивними та гібридними технологіями [1].

Діяльність боротьбі з тероризмом окрім силової фази антитерористичної операції передбачає ще й проведення спеціальних заходів, спрямованих на попередження та запобігання злочинів терористичної спрямованості, при цьому, враховуючи ступінь інформатизації суспільства, особливої актуалізації це питання набуває стосовно віртуального простору та блогосфери.

Найважливішим компонентом блогосфери є соціальні мережі, які, наприклад, підчас нещодавніх подій на Близькому Сході використовувалися як головний компонент інформаційної зброї, засіб для порушення комунікаційного суверенітету держав і проведення акцій дезінформації, з метою спотворення духовно-моральних цінностей, руйнування цивілізаційного коду нації, руйнування системи безпеки держави, формування передумов терористичної діяльності. Поширення спеціально підібраної інформації в блогосфері особливо зростає в кризових ситуаціях. Це особлива форма ведення інформаційної війни, з використанням заздалегідь заготовленого дезінформаційного контенту, спеціально підготовлених інформаційних груп, що використовують методи масованої психологічної обробки учасників соціальних мереж і населення для поширення панічних настроїв та дестабілізації соціально-політичної обстановки в державі. Сенс терористично-мережевої війни якраз і полягає в формуванні громадської думки, громадських процесів, у випадку розповсюдження тероризму таким чином, щоб віртуальне співтовариство стало спільником у формуванні віртуального страху, без чого терористична діяльність малоефективна. Суспільство стає, таким чином, активним учасником терористичної діяльності [2, 5, 6].

Сучасний тероризм активно опановує мережеві технології та активно застосовує як ефективну зброю епохи мережевих війн, тому, на нашу думку, слід приділяти певну увагу моніторинговим технологіям отримання упереджувальної інформації про передумови соціальних конфліктів, що провокують тероризм та соціально-інформаційним заходам їх нейтралізації, активно використовуючи можливості мереженого інформаційного простору.

Якщо терористичну діяльність розглядати як різновид кризового явища соціального характеру, то технологія протидії має базуватися на застосуванні, насамперед, адекватних, що випливають з його інформаційної сутності, методів. Інформаційну протидію терористичній діяльності необхідно будувати на різних етапах її прояву, насамперед на етапі прихованої фази формування, віддаючи переваги заходам попереджувального характеру для забезпечення впливу на правосвідомість громадськості, представників окремих категорій або груп осіб, організацій, установ, підприємств та спеціальних служб іноземних держав з метою локалізації та нейтралізації негативних процесів, недопущення можливих небажаних наслідків, що можуть позначитися на рівні забезпечення національної безпеки, а також усунення причин і умов вчинення злочинів терористичної спрямованості [2, 3].

Профілактика тероризму – сукупність соціальних процесів, спрямованих на мінімізацію теророгенності соціальних систем шляхом проведення відповідних попереджувально-профілактичних заходів соціального, правового, виховного та іншого характеру. Їх головною метою є нейтралізація або усунення причин і умов вчинення тероризму, формування цілеспрямованого попереджувального впливу на осіб (груп осіб, організацій, рухів тощо) з антигромадською поведінкою, як в їх власних інтересах, так і в інтересах суспільства, а також спрямовані на зниження ризику для осіб стати жертвами терористичних (злочинних) посягань. Підставами для здійснення заходів профілактики є наявність достатньої інформації, що свідчить про наміри проведення спеціальними службами іноземних держав, а також організаціями, окремими групами (категоріями) реальних або віртуальних співтовариств терористичної діяльності, або провокації соціального конфлікту (передумов до цього), спроб створити такий контекст, щоб суспільство нормально або навіть позитивно сприйняло використання терористичних або екстремістських заходів при проведенні радикальних соціальних змін, неконтрольований розвиток яких може негативно вплинути на стан захисту державної безпеки. При цьому, особливу увагу слід приділяти саме віртуальним спільнотам, як потенційно-теророгенним [3, 4].

Здійснення інформаційного впливу в інтересах формування суспільної думки щодо засудження методів та ідеології тероризму, висвітлення спеціально підібраної інформації з метою нейтралізації теророгенності шляхом цільового інформаційного впливу на обраний об’єкт та контроль досягнення необхідного теророгенного ефекту може бути реалізовано за

допомогою патріотично налаштованих активних користувачів соціальних мереж. Подібні віртуальні спільноти можуть бути задіяні і у попередженні чи мінімізації суспільного резонансу соціального конфлікту через висвітлення резонансних подій та формування відповідної громадської думки, зокрема, й щодо формування позитивного іміджу спеціальних служб, позиціонування стратегій боротьби з тероризмом та тактики проведення антитерористичних операцій.

Як логічно витікає з вищенаведеного, профілактика тероризму в країні потребує негайного подальшого удосконалення. Протистояння терористичним загрозам можливе лише в тому разі, якщо сучасна українська спільнота, а не тільки представники спеціальних служб, виробить адекватну відповідну стратегію, на тому ж рівні технологічних уявлень про процеси, на якому ведеться терористично-мережева війна. Неможливо вибудувати адекватної відповіді викликам терористів без опанування блогосфери та аналогічних соціально-інформаційних віртуальних просторів як сфери впливу більш тонких технологічних концептів з використанням інноваційних інформаційних та мережевих технологій. Варто визнати, що стратегія профілактики тероризму має бути вибудувана не на рівні звичайних технологій протидії злочинності, а на більш серйозному, парадигмальному рівні.

Література

1. Війна на сході України [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Війна_на_сході_України.

2. Терроризм : определения и сущность : монография / [А.В. Коростыленко, Б.Д. Леонов, И.Н. Рыжов и др.] под общ. ред. В.В. Крутова, И.И. Мусиенко, В.А. Глушкова. – К. :Центр уч.-науч. и науч.-практ. изданий НА СБ Украины. 2014. – 192 с.

3. В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. - К.: Інтертехнологія, 2009. - 164 с.

4. Рижов І.М. Щодо необхідності формалізації профілактики тероризму/ Науковий вісник Ужгородського національного університету. Серія «Право».– 2014. – №29 том 2. – С.149-153

5. Мальцева Л. Українська блогосфера: функціонально-стильова характеристика / Лілія Мальцева / Вісник Львівського університету. Серія філологічна. 2011. Випуск 52. С.278-289

6. Keren M. Blogosphere : The new political arena / M. Keren. [Електронний ресурс]. – Режим доступу:

http:// www.lexingtonbooks.com/Catalog/SingleBook.shtml

ПРОВЕДЕННЯ ПОШУКУ ТОРГОВЕЛЬНИХ МАРОК З ЗАСТОСУВАННЯМ ОФІЦІЙНИХ БАЗ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Ромашко А.С., Литвин О.В., Кравець В.О.
ММІ НТУУ "КПІ"

На цей час в Україні на офіційному сайті Українського інституту промислової власності (УІПВ) надається доступ до різноманітних баз даних (БД) [1] та інформаційно-довідкових систем (ІДС), зокрема і до тих, що стосуються торговельних марок. Багато патентних фірм пропонують процедуру пошуку торговельної марки. Для якісного пошуку також можна звернутисть до Філіалу Державного підприємства «Українського інституту промислової власності» - Українського центру інноватики і патентно-інформаційних послуг [2].

На сайті УІПВ можна також здійснити і самостійний пошук за такими базами даних: БД "Зареєстровані в Україні знаки для товарів і послуг"; БД "Відомості про добре відомі знаки в Україні"; БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність", БД "Заявки на знаки для товарів і послуг, прийняті до розгляду" (з'явилася в кінці літа 2015 р. і в цій статті не аналізувалась) .

В кожної з цих баз є свої можливості та обмеження. Загальним недоліком баз даних стосовно торговельних марок на сайті УІПВ, з точки зору споживача, є те, що в Україні не можна самостійно шукати інформацію за поданими заявками на торговельні марки. В цьому випадку існує так звана "мертва зона" пошуку, бо цілком можливий випадок, коли, наприклад, місяць тому була подана заявка на тотожну торгівельну марку і відшукати таку торговельну марку самостійно не можливо.

Для того щоб провести пошук торговельної марки по заявкам, потрібно звернутись до Українського центру інноватики і патентно-інформаційних послуг. Але ця процедура не безкоштовна [2], до того ж повної гарантії не має.

Характеристика баз даних, доступних на сайті УІПВ наведена в таблиці 1.

Пошук можна здійснити за БД «Зареєстровані в Україні знаки для товарів і послуг», але ця база (окрім нумераційного, іменного та пошуку за кольорами) передбачає можливість здійснення пошуку тільки за класами Міжнародної класифікації товарів та послуг для цілей реєстрації знаків (Ніццька класифікація) [3] і в результаті ми отримуємо досить значний масив інформації, який важко проаналізувати (наприклад, якщо нас цікавить торговельна марка для виробника виробів з металів та їх сплавів, в тому числі металоконструкцій, то нам слід здійснити пошук за класом 6 і станом на 01.09.2015 року ми отримали 6391 знаків).

Для більш швидкого пошуку потрібно скористатись базами даних, що передбачають можливість пошуку за ключовими словами та Міжнародною класифікацією зображувальних елементів знаків (Віденська класифікація) [4] а саме - БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про видачу свідоцтв України на знаки для товарів та

послуг". В пошуковому полі зазначимо одночасно коди Віденської класифікації та Ніццької класифікації і отримаємо менший масив торговельних маркок.

Таблиця 1

Бази даних на сайті УІПВ стосовно торговельних марок

Назва бази та її електронна адреса	Переваги	Недоліки
БД "Зареєстровані в Україні знаки для товарів і послуг" http://base.uipv.org/searchBUL/search.php?dbname=carttm	Інформація надається починаючи з бюлетеня 1/1993 Пошук нумераційний; Пошук іменний Пошук за Ніццькою класифікацією Пошук за кольорами	Відсутня можливість пошуку за заявками При пошуку за Ніццькою класифікацією отримуємо великий масив інформації Відсутня можливість пошуку за Віденською класифікацією та за ключовими словами
БД "Відомості про добре відомі знаки в Україні" http://base.uipv.org/searchBul/search.php?dbname=certwkm	Пошук нумераційний; Пошук іменний Пошук за типом рішення Пошук за ключовими словами Пошук за Ніццькою класифікацією	Відсутня можливість пошуку за Віденською класифікацією
БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про видачу свідоцтв України на знаки для товарів та послуг" http://base.uipv.org/searchBul/search.php?action=changedb	Пошук нумераційний; Пошук іменний Пошук за типом рішення Пошук за Ніццькою класифікацією Пошук за Віденською класифікацією Пошук за ключовими словами Пошук за кольорами	Інформація надається починаючи з бюлетеня 4/2006 Відсутня можливість пошуку за заявками Відсутня можливість пошуку за Мадридською системою
БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про знаки, зареєстровані відповідно до Мадридської угоди про міжнародну реєстрацію знаків та/або Протоколу до Мадридської угоди про міжнародну реєстрацію знаків"	Пошук нумераційний; Пошук іменний Пошук за типом рішення Пошук за Ніццькою класифікацією	Інформація надається починаючи з бюлетеня 4/2006 Відсутня можливість пошуку за заявками Відсутня можливість пошуку за Віденською класифікацією та за ключовими словами

Назва бази та її електронна адреса	Переваги	Недоліки
http://base.uipv.org/searchBul/search.php?action=changedb		
БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" Відомості про добре відомі знаки в Україні http://base.uipv.org/searchBul/search.php?action=changedb	Пошук нумераційний; Пошук іменний Пошук за типом рішення Пошук за ключовими словами Пошук за Ніццькою класифікацією	Інформація надається починаючи з бюлетеня 4/2006 Відсутня можливість пошуку за Віденською класифікацією

При застосуванні БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про видачу свідоцтв України на знаки для товарів та послуг", слід врахувати, що в ній наявна інформація з квітня 2006 року (а свідоцтво видається на десятирічний термін), до того ж щороку з цієї бази видаляються "старі" записи. Інформацію, якої не має у вищезазначеній базі можна шукати лише переглядаючи окремі бюлетені "Промислова власність", які теж існують в електронній формі. Такий пошук потрібно виконати стосовно усіх номерів бюлетенів до завершення десяти років на дату планованої подачі заявки (для процедури моніторингу на дату виконання моніторингу). Для пошуку по бюлетеням за БД «Зареєстровані в Україні знаки для товарів і послуг» набираємо, наприклад, бюлетень 3/2006 та клас 6 Ніццької класифікації, результат - 25 торговельних марок.

При застосуванні БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про видачу свідоцтв України на знаки для товарів та послуг", слід врахувати, що в ній відсутня інформація про діючі в Україні свідоцтва за Мадридською системою, тому можливі такі варіанти:

- потрібно звернутись до іншої БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність", а саме до БД "Відомості про знаки, зареєстровані відповідно до Мадридської угоди про міжнародну реєстрацію знаків та/або Протоколу до Мадридської угоди про міжнародну реєстрацію знаків". Набираємо клас 06 Ніццької класифікації, результат – 2146 торговельних марок (знову ж таки великий обсяг інформації), тому доцільно використати БД «ROMARIN», яка розміщена на сайті Всесвітньої організації інтелектуальної власності [5], для пошуку торговельних марок, що діють в Україні за Мадридською системою;
- потрібно звернутись до БД "Відомості про добре відомі знаки в Україні". Набираємо клас 06 Ніццької класифікації, результат – 4 торговельні марки. Оскільки існує вірогідність того, що на час перевірки знак, який наявний в цій базі не визнаний добре відомим в Україні (з часом ситуація може змінитися не на

користь власника ТМ в Україні), тому слід звернутись до Глобальної бази даних по брендам [6].

Висновки і пропозиції

Рекомендумо здійснювати пошук торговельної марки планованої до реєстрації чи вже зареєстрованої (для моніторингу) у такій послідовності:

1. Визначити коди за Ніццькою угодою про Міжнародну класифікацію товарів і послуг для реєстрації знаків (Ніццька класифікація).

2. Визначити коди зображальних елементів знаків за Міжнародною класифікацією зображувальних елементів знаків (Віденська класифікація).

3. Здійснити пошук за базами даних на сайті УІПВ

3.1 За БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" "Відомості про видачу свідоцтв України на знаки для товарів та послуг" за кодами Віденської класифікації.

3.2 За БД "Електронна версія акумулятивного офіційного бюлетеня "Промислова власність" Відомості про добре відомі знаки в Україні за кодами Ніццької та Віденської класифікації.

3.3. За БД "Зареєстровані в Україні знаки для товарів і послуг" по окремим бюлетням до закриття 10-ти річного циклу за кодами Ніццької класифікації.

3.4 За БД "Заявки на знаки для товарів і послуг, прийняті до розгляду".

4. Здійснити пошук за базами даних на сайті за БД "BOIB".

4.1. За БД"ROMARIN":

- якщо не планується міжнародна реєстрація, то за ключовими словами, кодом держави Україна згідно із стандартом BOIB ST.3 та за кодами Ніццької та Віденської класифікації;

- якщо планується міжнародна реєстрація, то за ключовими словами, за кодами Віденської класифікації, та будь-якими доступними даними (наприклад за кодами "потрібних" держав згідно із стандартом BOIB ST.3).

4.2. За Глобальною базою даних по брендам, з урахуванням доцільності планування/наявності міжнародної реєстрації торговельної марки.

5. За БД патентних відомств окремих країн, в яких планується/наявна реєстрація торговельної марки.

Література

1. Бази даних та інформаційно-довідкові системи /Український інститут промислової власності (УІПВ). [Електронний ресурс]. – Режим доступу: http://www.uipv.org/ua/bases2.html.

2. ЗНАКИ ДЛЯ ТОВАРІВ І ПОСЛУГ (ТОРГОВЕЛЬНІ МАРКИ)/ Український центр інноватики та патентно-інформаційних послуг [Електронний ресурс]. – Режим доступу: http://iii.ua/uk/znaki-dlya-tovariv-i-poslug-torgovelni-marki

3. ІДС "Міжнародна класифікація товарів і послуг для реєстрації знаків (Ніццька класифікація). Десята редакція, версія 2015 року". [Електронний ресурс]. – Режим доступу: http://nice102015.uipv.org/.

4. ІДС "Міжнародна класифікація зображувальних елементів знаків (Віденська класифікація). Сьома редакція". [Електронний ресурс]. – Режим доступу: http://base.uipv.org/vienna7/

5. ROMARIN / Всемирная организация интеллектуальной собственности [Електронний ресурс]. – Режим доступу: http://www.wipo.int/madrid/ru/romarin/,

6. Глобальная база данных по брендам / Всемирная организация интеллектуальной собственности [Електронний ресурс]. – Режим доступу: http://www.wipo.int/reference/ru/branddb/.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ЗАСІБ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Сірик А.О.
Міністерство оборони України

Одним з основних чинників успішності дій під час ведення збройної боротьби є домінування в інформаційному просторі. За сучасними концептуальними поглядами провідних країн світу і згідно з керівними документами їх державних структур боротьба в інформаційній сфері спрямована на завоювання інформаційної переваги. Інформаційна перевага полягає в досягненні переваги в інформаційно-психологічній та інформаційно-технічній сферах. Для держав, у яких є концепція ведення інформаційних кампаній, операцій і які володіють сучасними інформаційними технологіями та розвиненою інформаційною інфраструктурою, інформаційну перевагу забезпечено ще на початковому етапі протистояння.

Серед сукупності засобів масової інформації (радіо, телебачення, друковані видання тощо), за допомогою яких здійснюється інформаційний вплив на цільову аудиторію, мережа Інтернет має свої особливості:

- висока мобільність – можливість використання інформаційних ресурсів миттєво в будь-якому місці за допомогою необхідних технічних пристроїв. Побачив, сфотографував, виклав на сайт. Поки телебачення підготує сюжет, Інтернет вже збере тисячі людей;
- можливість одночасного спілкування безлічі людей на різних кінцях світу;
- свобода слова – це феномен в якому Інтернет стає не тільки правомірним підґрунтям, де кожна людина може написати все, що захоче, а й місцем для вільного викладення своїх думок;
- кожна віртуально-соціальна спільнота в найкоротші терміни може змінити свій вид, форму існування і діяльності. Через труднощі встановлення зв'язку між віртуально-соціальними спільнотами мережі Інтернет та іншими суб'єктами інформаційної боротьби майже неможливо довести юридичну провину спільноти за вчинені нею дії і відповідно притягти її до відповідальності.

Практичне застосування Інтернет-простору для виконання завдань інформаційної боротьби в основному полягає в оперативній передачі та отриманні інформації. Останнім часом найпоширенішим об'єктом і одночасно засобом ведення інформаційних операцій є соціальні мережі.

Поняття “соціальні мережі” вперше ввів соціолог Джеймс Барнс: “Соціальна мережа (Social Network) – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними”.

Розвиток соціальних мереж в Інтернет-просторі почався в 1995 році з американського порталу Classmates.com. Проект виявився настільки успішним, що в наступні кілька років спровокував появу не одного десятка аналогічних сервісів. Але офіційним початком буму соціальних мереж прийнято вважати 2003–2004 роки, коли були введені в дію Linkedin, MySpace і Facebook.

Соціальні мережі (наприклад: Facebook, Twitter, Vkontakte, Одноклассники тощо) стали одним з важливих інструментів інформаційного впливу, в тому числі з метою маніпулювання особистістю, соціальними групами і суспільством в цілому.

З початком воєнного конфлікту різко підвищується активність користувачів соціальних мереж – прихильників з обох протиборчих сторін в мережі Інтернет. Мета організаторів спільноти в соціальних мережах, насамперед, полягає в підтримці і консолідації в мережі всіх, хто підтримує і поширює для їх багатомільйонного сегмента політичні та стратегічні погляди не стільки серед лояльних інтернет-користувачів, скільки серед нейтральних користувачів, а також супротивників. Головне завдання спільноти – ініціювати та координувати роз'яснювальну роботу по своїй позиції, використовуючи інформаційну пропаганду і дуже часто дезінформацію.

Щоб брати участь в інформаційній боротьбі, не обов'язково бути хакером, журналістом, звичайним блогером або блогером з особливим статусом, що на договірних засадах освітлює ті чи інші події, досить мати свій акаунт в будь-якій соціальній мережі. Приклад тому – активне протистояння російських та українських звичайних користувачів Інтернет під час анексії Криму та захоплення територій Донецької і Луганської областей України з метою формування не лише громадської думки а й формування переконань.

Основними особливостями використання соціальних мереж під час ведення інформаційної боротьби у воєнних конфліктах останнього десятиріччя є:

1. Інформаційні повідомлення формуються шляхом природного відображення дійсності в ході безпосереднього спілкування учасників будь-яких подій і поширення ними інформації різній аудиторії, а також формування інформаційних заходів, які підготовлені завчасно відповідними фахівцями.

2. Розкручування інформаційних ситуацій до критичного рівня дає змогу спровокувати суспільство на активні дії (до масових протестів). Здійснюється воно шляхом впливу на інформацію, що циркулює в соціальних мережах, а саме: поширення чуток, підготовка відомостей, що підтверджує або спростовує ту чи іншу подію з метою формування у суспільстві необхідних настроїв, поглядів, переконань.

3. Настрої в реальний світ переносяться в результаті інформаційного впливу на мотиваційну основу особистостей, у яких уже були певні

погляди, що необхідні для реалізації тих чи інших намірів суб'єктів впливу. У результаті інформаційного впливу на групи населення і конкретних осіб з нестійкими поглядами можливо змінити їх соціальну поведінку.

4. Створення інформаційної обстановки і провокування суспільства на активні дії змушує воєнно-політичне керівництво країни-противника ухвалювати неправильні, непрофесійні рішення. Цим самим формується думка у суспільстві щодо відсутності компетенції осіб, які приймають рішення. Це може спровокувати відсторонення або обмеження повноважень окремих керівників. Такими провокаціями добиваються сковування ініціативи керівництва різного рівня або формування громадської думки і настроїв, що перешкоджають роботі органів державної влади.

Таким чином, соціальні мережі є ареною сучасних інформаційних кампаній, операцій як основних форм ведення інформаційної боротьби і засобом супроводу різних військових і політичних процесів протиборчих сторін.

Активне використання соціальних мереж дає змогу оперативно впливати на думку і поведінку людей, що призводить до протистояння груп з різнорідними інтересами. Масштаби впливу на людей та управління подіями відкриває перед мережами великий спектр вирішуваних завдань. У зв'язку з відсутністю цензури і різного роду перешкод користувачі мереж діють як на передовій, створюючи сприятливу основу успішного функціонування у віртуальному і реальному просторі. Все це перетворює соціальні мережі на один із важливих інструментів досягнення інформаційної переваги над противником.

МЕТОД ВЫДЕЛЕНИЯ ПОДСЕТЕЙ В КАЗУАЛЬНЫХ СЕТЯХ В ЗАДАЧАХ СЦЕНАРНОГО АНАЛИЗА

Снарский А.А., Ландэ Д.В.
ИПРИ НАН Украины, НТУУ «КПИ»

При проведении сценарного анализа во многих областях, например, в области безопасности, рассматриваются онтологии соответствующих предметных областей [1]. В частности, качестве узлов графа рассматриваемой онтологии могут выбираться факторы безопасности (объекты, субъекты, угрозы, уязвимости и т.п.), а в качестве связей – причинно-следственные связи между факторами (граф с направленными ребрами). Узлам и связям приписываются числовые значения, которые в дальнейшем могут корректироваться. Связи могут быть как положительными (увеличение значения первого фактора приводит к увеличению значения второго фактора), так и отрицательными (увеличение значения первого фактора приводит к уменьшению значения второго фактора) [2]. Онтологии, как правило, создаются экспертами, а также возможно автоматизированное создание онтологий на основе анализа соответствующих текстовых массивов [3]. В последнем случае предполагается постоянная актуализация значений факторов безопасности и связей между ними в зависимости от объемов и содержания сообщений, появляющихся в целевом фрагменте информационного пространства [4], и знаний экспертов.

Сценарии информационной поддержки, как правило, связываются с определенными факторами безопасности (объектами или субъектами и уязвимостями). Для построения сценариев обеспечения безопасности того или иного объекта предполагает, что после выбора целевых факторов сценария в графе онтологии выявляются подграфы (частичные онтологии), наиболее тесно связанные с выбранным объектом.

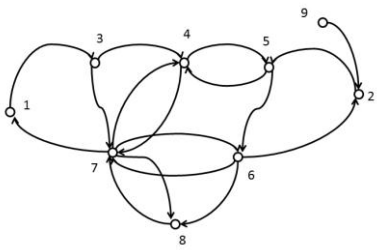
При решении этой задачи решающим фактором оказывается определение силы связи между отдельными узлами онтологии – между отдельными факторами безопасности, в рассматриваемом случае.

В рассматриваемой сети узлы связаны между собой связями, отражающими влияние одного узла на другой. Каждой связи приписано две характеристики: первая – направление влияния, вторая – величина влияния (рис. 1а).

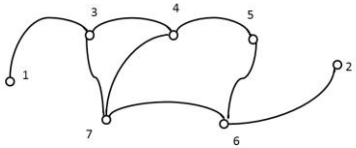
Так например, узел 1 напрямую влияет на узел 3, но узел 3 напрямую на узел 1 не влияет.

Кроме того, каждой связи, задающей влияние, соответствует ее величина. Например, для связи между узлами 1 и 3 это влияние задается как число ε_{13}, которое может быть как положительным, так и отрицательным.

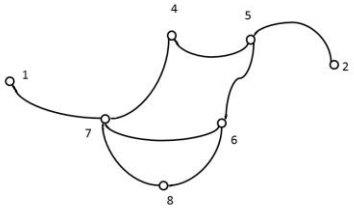
Для решения задачи определения взаимного влияния узлов кажется естественным применение законов электротехники. Вместе с тем, подход опирающийся на непосредственное применение закона Кирхгофа приводит к некоторому логическому противоречию. В некоторых схемах влияние узла 1 на узел 2 $\varphi(1 \to 2)$ зависит от влияния узла 2 на узел 1 $\varphi(2 \to 1)$.



а



б



в

Рис. 1. Пример сети влияния: *а* – общая направленная сеть; *б* – подсеть влияния узла 1 на узел 2; *в* – подсеть влияния узла 2 на узел 1

Поэтому авторами был предложен алгоритм определения величины влияния одного узла (например, 1-го) на другой (например, 2-й), состоящий из двух частей. Вначале необходимо выделить ту часть сети, по которой осуществляется влияние первого узла на второй. Для этого из начальной сети (рис. 1 а) нужно удалить все связи, оставляя только те, по которым

можно пройти из первого узла во второй (рис. 1*б*). Аналогично выделяется сеть влияния второго узла на первый (рис. 1*в*). Отметим, что в общем случае сети, изображенные на рис. 1*б* и 1*в*, не совпадают.

После выделения подсетей (подсети $1 \to 2$ и $2 \to 1$) используем аналогию с электрическими сетями. Величина влияния $i-$го узла на $j-$й ε_{ij} в данной аналогии – это ЭДС. Сопротивление каждой связи в рамках данного допущения принимается равным 1. Распределение токов – J_{ij}, текущих по связям ij, определяется решением уравнения Кирхгофа:

$$\forall k: \sum_{i \to k \to j} J_{ij} = 0, \quad \forall z: \sum_{i,j \in z} J_{ij} = \sum_{i,j \in z} \varepsilon_{ij},$$

где первое уравнение требует (для стационарного случая), чтобы алгебраическая сумма токов в каждом узле k была равной нулю, а второе, чтобы для любого замкнутого контура z сумма токов (с учетом того, что сопротивление всех связей равно единице) было равно сумме всех ЭДС ε_{ij} в этом же контуре.

После решения системы уравнений (1) и нахождения токов J_{ij} выбирается любой контур, соединяющий узлы 1 и 2, например, контур 1-3-4-5-6-2 и из уравнения Кирхгофа для незамкнутого контура:

$$\sum \varepsilon + \varphi_1 - \varphi_2 = \sum J,$$

находится разность потенциалов $\varphi_1 - \varphi_2$ (суммирование производится по связям выбранного контура).

Аналогично происходит вычисление для любых других пар узлов.

Именно поэтому для нахождения влияния одного узла на другой расчет приводится в соответствии с несколько измененной схемой, соответствующей рис. 1*а*–1*в*. На первом шагу от направленной сети (рис. 1*а*) происходит переход к ненаправленным подсетям (рис. 1б и 1в). Итак, на первом шаге происходит модификация направленной сети связи. После выбора узлов, для которых изучается взаимное влияние, остаются только связи, по которым можно пройти от одного узла к другому (рис. 1*б* и 1*в*).

На втором шаге происходит расчет $\varphi(1 \to 2)$ происходит по правилам Кирхгофа (рис. 1б). Естественно, при расчете влияния узла 2 на узел 1 расчет происходит по другой схеме (рис. 1*в*). При этом связи считаются обычными проводниками с единичным сопротивлением, и в $\varphi(\alpha \to \beta) = \varphi(\beta) - \varphi(\alpha)$ принимается $\varphi(\alpha) = 0.$ Заметим, что при таком методе расчета влияние узла 1 на 2 не зависит от влияния узла 2 на 1.

Далее предложенный метод расчета распадается на два сценария.

Сценарий I:

В модифицированной сети удаляется узел α, после чего опять производится расчет и находится $\varphi(\beta)^I$. Величиной влияния узла α на β считается величина:

$$V_{\alpha\beta}^I = \varphi(\beta) - \varphi(\beta)^I. \quad (5)$$

Сценарий II:

В модифицированной сети удаляется узел α и все удаляемые с ним связи, после чего производится расчет $\varphi(\beta)^{II}$. Величиной влияния узла α на β в этом случае считается величина:

$$V_{\alpha\beta}^{II} = \varphi(\beta) - \varphi(\beta)^{II}.$$

Таким образом, фактически предложены два похода к вычислению взаимных влияний между узлами в основной сети, которая может трактоваться как сеть причинно-следственных связей между объектами в заданной предметной области. В случае задачи, связанной с обеспечением безопасности некоторого объекта, соответствующего узлу, из общей казуальной сети выбираются узлы-объекты, имеющие наибольший вес связи с целевым объектом. Выделение подсетей из данных узлов и целевого узла, а также связей между ними, определение планов очередности влияния на эти подсети, задает сценарии информационной поддержки, в частности, в задачах принятия решений в области безопасности.

Литература

1. Боргест Н.М. Научный базис онтологии проектирования // Онтология проектирования. – 2013. №1(7). – С.7-25.
2. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Структурно-динамический подход к сценарному анализу процессов информационного противоборства в Арктике // Труды XII Всероссийского совещания по проблемам управления (ВСПУ 2014). – М.: ИПУ РАН, 2014. – С. 8889-8901.
3. Д.В. Ландэ, А.А. Снарский. Подход к созданию терминологических онтологий // Онтология проектирования, 2014. № – 2(12). – С. 83-91.
4. 1.Kleinberg J. Temporal dynamics of on-line information streams // Data Stream Management: Process-ing High-Speed Data Streams. — Springer, 2006. –18 p.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПАТЕНТУВАННІ ВИНАХОДІВ (КОРИСНИХ МОДЕЛЕЙ)

Струтинський В.Б., Ромашко А.С., Богиня К.О.
ММІ НТУУ "КПІ"

Статтею 12 Закону України [1] визначено, що формула винаходу (корисної моделі) "повинна виражати його суть, базуватися на описі і викладатися у визначеному порядку ясно і стисло", а опис винаходу (корисної моделі) "повинен викладатися у визначеному порядку і розкривати суть винаходу (корисної моделі) настільки ясно і повно, щоб його зміг здійснити фахівець у зазначеній галузі".

Після отримання патенту (в певних випадках до отримання) інформація публікується, тобто стає відкритою, а це значить, що фахівець конкурента може відтворити за описом, формулою та кресленнями пристрій чи спосіб.

Виходячи з вищесказаного при патентуванні існує потенційна небезпека, що об’єкт буде використаний (наприклад виготовлений чи застосований) третіми особами.

Тобто наша задача полягає в тому, щоб отримати охоронний документ у відповідності до вимог Закону і при цьому частину інформації зберегти нерозкритою. Це особливо важливо в плані національної безпеки на сьогодні, оскільки в Україні активізувалась технічна творчість оборонній галузі і не завжди інформація, що патентується засекречується.

За результатами пошуку за базою даних "Спеціалізована БД "Винаходи (корисні моделі) в Україні" [2] станом на 01.09.2015 знайдено:

- за кодом МПК F41 – "ЗБРОЯ" - **1296** патентів.
- за кодом МПК F42 – "БОЄПРИПАСИ; ПІДРИВНІ РОБОТИ" - **1035** патентів.

Серед знайдених патентів є такі, що стосуються гірництва, є діючі патенти, є не діючі, а також зустрічаються окремі патенти іноземних фірм. Усі знайдені патенти надані з описами патентів та дуже часто з кресленнями. Але є ще й інші коди МПК, в яких може бути інформація, яку варто засекретити.

Слід зазначити, що є патенти, які зареєстровані на ім'я фізичних осіб, і кому свій патент ця особа продасть в майбутньому – невідомо. Також не відомо як це відобразиться на обороноздатності нашої країни. Та й доля самих патентувальників таких винаходів (якщо винайдено щось, що дійсно варте уваги) може бути під загрозою і не зрозуміло чому такі особи не використовують можливість не відкривати своє ім'я, хоча це передбачено бланком заяви на отримання патенту.

Після подачі заявки перед проведенням експертизи у відповідності до статті 16 Закону України [1], будь-яка заявка українських резидентів (навіть та на яку не оформлюється заява про секретний винахід чи корисну модель), що проходить попередню експертизу "розглядається на предмет наявності в

ній відомостей, які можуть бути віднесені згідно із Зводом відомостей, що становлять державну таємницю, до державної таємниці". Тим не менше в галузі озброєння та боєприпасів зустрічаються патенти видані у 2014 та 2015 роках (дані факти не аналізувались і можливо наявність таких патентів пов'язана зі змінами до "Зводу відомостей, що становлять державну таємницю" [3], останні з яких здійснювались у 2014 та у 2015 роках).

Прямо говорити про наявність секретної інформації в матеріалах заявки, зокрема у формулі, не можна, бо ви тим самим "підписуєтесь" під тим, що не досить ясно та повно розкрили суть, див. "Правила складання і подання заявки на винахід та заявки на корисну модель" - далі Правила складання [4, п. 6.8.2, 6.8.3, 7.1.3], і така заявка може бути відхилена, або, у випадку видачі патенту, довести факт порушення прав власника патенту буде неможливо.

Деякі заявники прямо зазначають у формулах своїх винаходів (корисних моделей) ознаки, які не можуть бути ідентифіковані чим порушують Правила складання [4], зокрема:

- назви речовин, які є невідомі на дату подання заявки;
- прямо зазначають вказівку на те, що певна інформація є секретною (наприклад. Для здійснення способу "…посилають надвисокочастотні сигнали, що носять дискретний характер (ноу-хау)";
- параметри пристрою у вигляді змінних (наприклад. "Елементи розташовані пуд кутом β один до одного");
- зазначають технічний результат замість ознак (наприклад. Пристрій .., який відрізняється тим, що дозволяє швидко вимірювати величину .. і підвищити зручність використання та достовірність вимірювань ..".

В будь-якому випадку навіть при патентуванні об'єктів, які не відносяться до державної таємниці для попередження незаконного користування патентом слід здійснити певні кроки, які не суперечать Правилам складання [4], а саме:

- надмірно не деталізувати суттєві ознаки винаходу чи корисної моделі, які стосуються форми реалізації окремих конструктивних елементів та зв'язків між ними;

- не розкривати в описі оптимальний склад речовини для досягнення найкращого технічного результату при зазначенні у формулі діапазонів складових, а в описі слід наводити окремі (не оптимальні) приклади реалізації речовини;

- не розкривати в описі оптимальні умови здійснення способу для досягнення найкращого технічного результату, з зазначенням у формулі діапазонів, наприклад режимів, а в описі окремі приклади (не оптимальні) реалізації способу.

В Правилах складання [4] немає прямої вказівки на те, що в розділі „відомості, що підтверджують можливість здійснення ..." має бути зазначена інформація достатня для досягнення найкращого технічного результату, але

така вказівка є в Угоді про торговельні аспекти прав інтелектуальної власності [5] і здійснюючи процедури набуття за межами України, заявник має бути готовий до цього. Наводимо витяг з Угоди про торговельні аспекти прав інтелектуальної власності [5, стаття 29, пункт 1]:

Члени повинні вимагати від заявників, які бажають одержати патент, щоб вони розкривали суть свого винаходу достатньо ясно і повно з тим, щоб кваліфікована у відповідній галузі особа могла використати винахід, а також можуть вимагати від заявників вказати найкращий відомий їм спосіб використання винаходу на дату подання заявки або при домаганнях на пріоритет - на дату пріоритету.

Тобто поки мова йде про державу Україна – „найкращий відомий … спосіб використання винаходу“ зазначати не обов'язково і саме тут може бути „схована“ інформація, яка є секретною.

Висновки

1. Доцільно ще раз переглянути процедуру перевірки на наявність в матеріалах заявки на патент Державної таємниці (зокрема щодо заявок на зброю та боєприпаси), можливо слід:

- засекречувати усі патенти, що відносяться до обороноздатності;
- проводити (щодо заявок на зброю та боєприпаси) обов'язкову перевірку новизни та промислової придатності навіть для корисних моделей;

2. Винахіднику слід визначити доцільність згадування свого імені при публікації відомостей стосовно заявки на видачу патенту.
3. Використати усі можливості для нерозголошення найкращого відомого заявнику/винахіднику способу використання винаходу (корисної моделі).

Література

1. Закон України "Про охорону прав на винаходи і корисні моделі". [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3687-12.
2. "Спеціалізована БД "Винаходи (корисні моделі) в Україні" [Електронний ресурс] – Режим доступу: http://base.uipv.org/searchINV/
3. Звід відомостей, що становлять державну таємницю. [Електронний ресурс] – Режим доступу http://zakon1.rada.gov.ua/laws/show/z0902-05
4. Правила складання і подання заявки на винахід та заявки на корисну модель». [Електронний ресурс] – Режим доступу http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0173-01&print=1.
5. Угода про торговельні аспекти прав інтелектуальної власності [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/981_018 .

ДОСЛІДЖЕННЯ КРИТЕРІЇВ ЦЕНТРАЛЬНОСТІ В ІЄРАРХІЧНИХ МЕРЕЖАХ

Сулема О. К., Ланде Д. В.
НТУУ «КПІ», ІПРІ НАН України

У багатьох прикладних галузях та сферах науки і техніки задачі аналізу топології мережі та дослідження особливостей її вузлів мають досить важливе значення. Зокрема, до таких галузей можна віднести інформаційну безпеку [1], організаційне управління, термінологічні онтології, генеалогічні дослідження тощо. Саме тому задачі, пов'язані з аналізом графів мереж, є та залишатимуться актуальними ще на довгий період часу.

Постановка задачі

Для визначення та оцінювання критеріїв центральності для графів ієрархічних мереж необхідно вирішити наступні підзадачі:

- визначення характеристик центральності у графах;
- аналіз алгоритмів та підходів обчислення визначених характеристик центральності;
- розроблення власних критеріїв центральності відповідно до практичних задач;
- постановка та розв'язання задачі багатокритеріальної оптимізації з метою оцінювання різних критеріїв.

Критерії класифікації графів

У теорії графів існує досить велика кількість різних характеристик центральності. Кожна з них може розглядатись залежно від поставленої практичної задачі. Відповідно, можна виділити групи таких характеристик, які будуть давати найкращий аналітичний результат з точки зору задачі, що розглядається:

- центроїдність;
- центральність за ексцентриситетом;
- мінімальний середній шлях;
- максимальний степінь;
- мінімальна кількість рівнів.

Для обчислення характеристик вузлів графа необхідно обчислювати матрицю відстаней, для чого існує багато алгоритмів пошуку на графах, серед яких найвідоміші – алгоритм Дейкстри, Беллмана-Форда, Флойда-Уоршелла, Джонсона [2, 3].

Для подальшої роботи було обрано алгоритм Флойда-Уоршалла, оскільки він, по-перше, дозволяє ефективно працювати з незваженими графами, які саме і досліджуються у цій роботі, а по-друге, знаходить

найкоротші шляхи між всіма вершинами, на виході даючи зведену матрицю відстаней.

Слід також зазначити, що матриця суміжності для ієрархічного графа має східчастий вигляд (рис. 1).

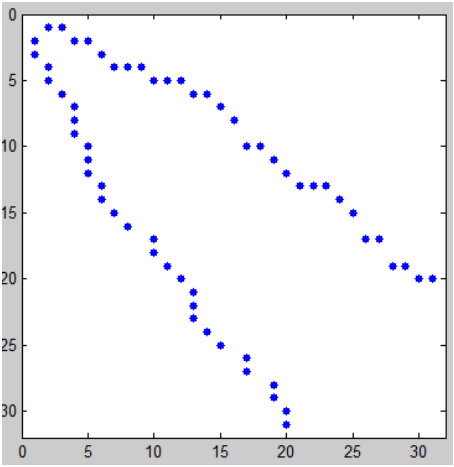


Рис. 1 – Матриця суміжності ієрархічного графа

Першою характеристикою, яка потенційно може бути одним з необхідних критеріїв центральності вузла, є центроїдність [4]. За означенням, центроїд графа складається з множини центроїдних вершин. Вершина v називається центроїдною відносно до дерева T, якщо v має найменшу вагу. Для її обчислення було розроблено алгоритм визначення ваги вершини шляхом знаходження всіх піддерев заданого дерева. За означенням, вагою вершини v називається найбільша кількість ребер по всім гілкам до даної вершини, де гілкою до вершини v є максимальне піддерево вихідного дерева T, що містить v як висячу вершину.

Другим розглянутим критерієм центральності є характеристика центральності за ексцентриситетом. Для її обчислення визначаються ексцентриситети всіх вершин дерева. За означенням, ексцентриситет – це максимальна з відстаней від даної вершини до всіх інших вершин [4]. Для обчислення ексцентриситетів застосовується матриця відстаней. За означенням, центральною вершиною графа G є така вершина v, для якої виконується вираз $e(v) = r(G)$, тобто ексцентриситет даної вершини дорівнює радіусу графа, що розглядається. Центр графа складається з множини центральних вершин, яких може бути одна чи дві.

Третім розглянутим критерієм центральності є значення мінімального середнього шляху [5]. Для обчислення даної характеристики також застосовується матриця відстаней, знаходиться середній шлях для всіх вершин заданого графа шляхом підрахунку середнього арифметичного для кожного рядка матриці відстаней. Ознакою центральності у цьому випадку є найменша середня відстань від деякої вершини v до всіх інших вершин графа, тобто мінімум з множини усіх середніх шляхів.

Четвертим критерієм центральності, що розглядався, є максимальний степінь вершини. Для його обчислення у матриці суміжності підраховується кількість одиниць у рядку, що відповідає заданій вершині. Остаточно обирається вершина, що відповідає максимуму у множині степенів всіх вершин графу.

П'ятим із розглянутих критеріїв центральності є кількість рівнів у графі. Дана характеристика обчислюється як максимальний із шляхів від кореня графа до всіх висячих вершин. Для його обчислення для кожного рядка матриці відстаней визначається максимальна відстань, а серед множини отриманих значень – мінімальне з них. Таким чином, вершина, для якої максимальна відстань є мінімальною, є найоптимальнішою вершиною за цим критерієм.

Аналіз критеріїв

Другий та п'ятий критерії можуть бути розглянуті як один критерій, оскільки їх математичний зміст є еквівалентним. Сформулюємо це як теорему. Відповідно доведено теорему: критерій центральності за ексцентриситетом та критерій мінімальної кількості рівнів є еквівалентними.

Також слід зазначити, що критерій центроїдності може бути застосований лише для ієрархічного графа, оскільки в такому графі немає циклів. Тобто для дослідження графів квазіієрархічної структури даний критерій не призначений. Але результат проведення 117 експериментів показав, що значення критеріїв центроїдності та мінімального середнього шляху завжди співпадають.

Таким чином, із розглянутих критеріїв центральності у полі зору авторів залишилося три основні:

- критерій мінімального середнього шляху;
- критерій максимального степеня;
- критерій мінімальної кількості рівнів.

Наведемо результати експериментальних досліджень ієрархічних графів невеликої розмірності, що підтверджують нерівнозначність даних критеріїв.

Експерименти проводились над групою ієрархічних графів, яка складається з 13 псевдовипадкових графів різної розмірності у діапазоні 15-33. Для кожного графу були застосовані критерії, в результаті чого була отримана множина оптимальних вершин за кожним з критеріїв.

На основі аналізу отриманої таблиць можна зробити висновок, що запропоновані критерії дійсно є рівноправними: у вибірці з 13 графів для

кожного з них результати критеріїв (оптимальна за даним критерієм вершина) є різними, а отже дані критерії не є еквівалентними одне одному.

Отже, у загальному випадку критерії центральності дають різні результати для графу, що аналізується. Одночасно вони є рівнозначними з точки зору пріоритетності, тому при отриманні декількох різних оптимальних вершин за даними критеріями неможна виділити один критерій, просто відкинувши інші. Тому для отримання єдиного розв'язку поставленої практичної задачі можуть бути методи багатокритеріальної оцінки, зокрема, метод пошуку оптимуму за Парето [6].

Підхід Парето полягає у наступному. Визначаються критерії, за якими відбуватиметься оцінка вершин графа. Складається таблиця, рядки якої – це відповідні критерії, а стовпці – номера вершин. Комірки даної таблиці заповнюються відповідними значеннями критеріїв для кожної вершини графа, що аналізується.

При порівнянні вершин за критеріями замість принципу «краще» використовується принцип «не гірше» за всіма критеріями. Формально, даний процес можна описати наступним чином.

Якщо i-та вершина гірша за j-ту вершину хоча б за одним критерієм при однакових інших, то дана i-та вершина викреслюється. Але у випадку, якщо хоча б за одним критерієм i-та вершина гірша за j-ту при тому, що за одним чи декількома іншими вона краща, то залишаються обидві вершини. В результаті, множина таких невикреслених вершин й складатиме множину Парето.

Як правило, отримана множина Парето складається з двох чи більше вершин. Для остаточного розв'язку підзадачі вибору кореня ієрархії необхідно визначити вершину, найоптимальнішу для практичної задачі, що розв'язується. Для цього можуть бути застосовані інші, орієнтовані на дану прикладну задачу методи.

Зокрема, можуть бути застосовані «наївні» методи багатокритеріальної оптимізації, одним з яких є об'єднання всіх критеріїв в одну функцію пристосованості *Fitness* за допомоги лінійного співвідношення.

Таким чином, на заключному етапі оптимізації необхідно визначити якість остаточного розв'язку у вигляді зваженої суми, що характеризує задовільність критеріїв відповідно до практичної задачі, що розв'язується. Для цього було розглянуто три групи ваг критеріїв – для кожного з критеріїв.

Висновки

В результаті проведеного дослідження було визначено характеристики центральності у ієрархічному графі та проведено аналіз алгоритмів і підходів до обчислення цих характеристик центральності. Було розглянуто деякі з критеріїв центральності вершин та проаналізовано окремі графи, на прикладах показано, що не всі критерії є еквівалентними у випадку

ієрархічних графів. Разом з цим, математично доведено, що для ієрархічних графів критерій центральності за ексцентриситетом і критерій мінімальної кількості рівнів, а також критерій центроїдності і критерій мінімального середнього шляху можна вважати в загальному випадку еквівалентними. Були визначені методи багатокритеріального оцінювання центральності з метою отримання оптимального результату, що відповідає прикладній задачі.

Література

1. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.
2. Bellman R. On a Routing Problem [Текст] / Quarterly of Applied Mathematics. Vol. 16, No. 1, 1958. – P. 87-90.
3. Левитин А. В. Алгоритмы: введение в разработку и анализ [Текст] / Пер. с англ. С. Г. Тригуб, И. В. Красикова. – М. : Издательский дом «Вильямс», 2006. – С. 345-353.
4. Харари Ф. Теория графов [Текст] / Пер. с англ. и предисл. В. П. Козырева. Под ред. Г. П. Гаврилова. Изд. 2-е. – М. : Едиториал УРСС, 2003. – С. 51-53.
5. Зябиров, Э. В. Методы определения кратчайшего пути между вершинами графа [Текст] / Э. В. Зябиров, С. П. Токарев, Л. И. Федосеева // Успехи современного естествознания. – 2011. – № 7 – С. 113-114.
6. Luke S. Essentials of Metaheuristics. A Set of Undergraduate Lecture Notes. Zeroth [Текст] / Edition. Online Version 0.5. Пер. с англ. Ю. Цой. – 2009. – P. 1-4.

ОДЕРЖАННЯ ВАЖЛИВОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КОНКУРЕНТНОЇ РОЗВІДКИ ТА ПРОМИСЛОВОГО ШПИГУНСТВА

Цирфа Г.О.,
ФСП НТУУ «КПІ»

Сьогодні прогнозувати ситуацію у конкурентному середовищі стає все складніше. Доволі часто, досягаючи домінуючого становища на ринку, окремі компанії виходять далеко за рамки чесних конкурентних відносин, а у процесі злиття і поглинання (концентрації суб'єктів господарювання) конкурентна боротьба переходить в економічну і, навіть, політичну площину.

Ринкова система створює свободу економічного вибору, кожен в праві виробляти і продавати свій товар. В результаті виникає економічне змагання, змагання, що іменується конкуренцією. Конкуренція – це цивілізована форма боротьби за виживання, це потужний спосіб безперервного стимулювання виробників певного товару. Конкуренція є одним з найважливіших способів підвищення ефективності як цілої економічної системи, так і всіх її ланок.

Але поряд із позитивною характеристикою завжди слід пам'ятати, що конкуренція – це і найжорстокіша боротьба за виживання і у переважній більшості вона націлена на знищення конкурента за будь-яку ціну. Тому, задля того щоб бути успішною, сучасній компанії не достатньо просто добре знати бізнес – їй також потрібно бути в курсі справ своїх конкурентів і партнерів. Але без фахівців, безперечно, тут не обійтись. Зібрати і осмислити інформацію про всіх, хто оточує компанію на ринку, – справа не проста. І саме цьому сприяє конкурентна розвідка, яка збирає і осмислює інформацію про всіх, хто оточує компанію на ринку, і важливо те, що конкурентна розвідка збирає саме неочевидну (скриту) інформацію. Мета діяльності конкурентної розвідки це аналіз і систематизація, здобутої чесними способами, інформації. Конкурентна розвідка – це перш за все, – маркетинговий інструмент вивчення конкурентного середовища, який є цілеспрямованим збором інформації про конкурентів для ухвалення управлінських рішень щодо подальшої стратегії та тактики ведення бізнесу.

У різних країнах простежуються різні трактовки терміну «конкурентна розвідка» і це пов'язано з особливістю доступу до інформації. Власне, конкурентна розвідка, принаймні у вигляді окремих її елементів, виникла одночасно з конкуренцією, але саме її поняття з'явилося набагато пізніше. Законодавче визначення поняттю «Конкурентна розвідка» в Україні поки що відсутнє. Натомість вважається вдалим визначення, запропоноване

Вікіпедією. Конкурентна розвідка - це постійний процес збору, нагромадження, структурування, аналізу даних про внутрішнє й зовнішнє середовище компанії та надання вищому менеджменту компанії інформації, що дозволяє йому передбачати зміни в обстановці і приймати своєчасні оптимальні рішення щодо управління ризиками, впровадження змін у компанії, а також відповідні заходи, спрямовані на задоволення майбутніх запитів споживачів та збільшення вартості компанії.

Якщо на заході культура бізнес-розвідки доволі розвинена і задіяна так що цей процес розуміється сам по собі то в Україні у цьому питанні ще досить багато непорозумінь. Проте, останні процеси економічного розвитку показали що і в Україні більшість великих компаній, не жалкуючи коштів, значну увагу приділяють організації й утриманню служби конкурентної розвідки. Щоб небажані несподіванки у роботі компанії майже не виникали, вона має постійно проводити моніторинг середовища, в якому працює.

Невід'ємною частиною бізнесу в Україні поступово стають і такі явища як промислове, комерційне, науково-технічне шпигунство (розвідка), а це означає, що конкурент дуже ретельно спостерігає за успішним (собі подібним) конкурентом, або за таким, що має важливу документацію. Як правило, це протиправні дії, спрямовані на збір, викрадання, накопичення цінної інформації тощо, що відбувається різними шляхами, І, нажаль, такі поняття як справедливість, чесність у конкурентному середовищі (бізнесі) дуже часто відходять далеко на останнє місце а натомість на передній план виходять такі правила за якими супротивники змушені грати в гру без правил, - діяти за принципом «переможців не судять», чи за принципом: «або ти - або тебе розорять і пустять з торбою по світу». Тому великі компанії не шкодують грошей і створюють розвідувальні структури. Ці структури повинні вчасно дізнатись про нечесні методи дій зацікавлених конкурентів і партнерів. Слід зазначити, що сучасний світ бізнесу все більше характеризується жорсткими конфліктами як на внутрішньому так і на зовнішньому ринку і дійовими особами тут вже виступають не тільки великі трести, корпорації, холдингові компанії тощо, а й окремі держави, які ревниво оберігають національну економіку.

Говорячи про конкурентну розвідку і промислове шпигунство, слід зазначити, що метою як однієї так і іншої структури є одержання інформації, яка б дала змогу здобути конкурентну перевагу на ринку. Вважається, що і розвідка і шпигунство вирішують наступні три завдання:

1) добування відомостей (легальним і нелегальним шляхом);
2) аналітична обробка відомостей;
3) доведення інформації до зацікавлених осіб.

Проте особливості кожної окремо полягають ось у чому. Поняття "шпигунство" відрізняється від поняття "розвідка" правовим статусом. Шпигунство ґрунтується переважно на незаконних методах отримання інформації, а розвідка - на законних.

Формально виникнення промислового шпигунства пов'язане із запровадженням у XVIII ст. системи патентів на винахід, які мали охороняти права винахідника чи дослідника. Промислове шпигунство (економічне, корпоративне шпигунство) має таке визначення: це - форма недобросовісної конкуренції, при якій здійснюється незаконне отримання, використання, розголошення інформації, яка являє собою комерційну, службову та іншу таємницю, що охороняється законом, з метою отримання переваг при здійсненні підприємницької діяльності, а, відтак, отримання матеріальної вигоди. Термін економічне, промислове, комерційне, науково-технічне шпигунство (розвідка) означає активні дії, спрямовані на збір, викрадання, нагромадження й обробку цінної інформації, закритої для доступу сторонніх осіб [1].

Перспективні фірми на протязі багатьох років приваблюють увагу шпигунів. Технології, данні клієнтів, корпоративні стратегії, все це цікавить не тільки конкурентів але і іноземні спецслужби. Все більше і віртуозніше хакери цілеспрямовано шукають лазівки у комп'ютерних системах. У спецслужб є відділи, які спеціалізуються на промисловому шпигунстві. Інтернет сьогодні широко розповсюджений, як і системи, які на ньому базуються. Багато підприємств представлені онлайн, вони підключені до всесвітньої мережі і через ці підключення хакери намагаються отримати доступ до інформації. Так, наприклад інтереси США в Німеччині стосуються перш за все військових концернів і їх угод. Зовсім недавно німецьку службу зовнішньої розвідки почали підозрювати у тому, що вона, вільно чи мимоволі, допомагала США шпигувати за підприємствами в Європі. Фахівці фірми m-prsvasi вважають, що великі компанії повинні зробити висновки з цього скандалу. Вони повинні захищати себе самі. Через шпигунський скандал довіра до державних структур дала тріщину, а може стала і зовсім підірваною. Якщо німецька спецслужба, яка повинна захищати підприємство всередині країни шпигує за ними на користь іноземної спецслужби то це серйозне зловживання довірою. Хто шпигує, за ким і чому? Коли мова заходить про промислове шпигунство, спецслужби часто діють на межі дозволеного [2].

До всього викладеного слід додати, що глобалізація економіки і подальше проникнення мережевих технологій в економіку, збільшення об'єму даних в Інтернеті, все це тільки грає на руку промисловим шпигунам, а розвиток інформаційних технологій і засобів їх застосування прискорюють

і примножують незаконні методи здобуття інформації. Тому у захисті важливої для будь якої компанії, а також держави, інформації слід застосовувати дієві технології, та засоби і методи боротьби, які вже закріплені в законодавстві Україні, та розробляти і затверджувати нові законодавчо-нормативні акти, які б затвердили нові правомірні методи і моделі боротьби, усунули прогалини і недоліки у цій важливій проблемі.

Литература

1. Навчальні матеріали онлайн / Режим доступу: http://pidruchniki.com/1319042042147/menedzhment/informatsiyna_bezpeka_obyektu_upravlinnya
2. Спецслужбы и промышленный шпионаж: Airbus обратится в суд / Режим доступу:https://www.youtube.com/watch?v=hX95UZOdFFA

АСПЕКТИ МАНІПУЛЯЦІЙ ЗМІ

Чернишина Г.Г.
ФСП НТУУ «КПІ»

На сучасному етапі розвитку людство стикається з різноманітними викликами, зокрема, соціальними. Та поряд із традиційними небезпеками і загрозами у XXI ст. з'явилася ще одна найпотужніша загроза - інформаційна. На сьогодні вона є чи не найвпливовішою та ефективною тому, що під її вплив все більше і більше підпадає майже все населення і контролювати її практично не можливо.

Кожен громадянин в правовій державі має право на приватне життя, яке включає в себе певну інформацію, яка не підлягає розповсюдженню. Однак, громадяни постійно зустрічаються з випадками, коли з них вимагають конфіденційні дані. Суб'єктів запевняють, що ці дані лише для службового використання та на що необхідно дати свою згоду. А також, в невідомий спосіб такі особисті дані стають публічними. Не всім це подобається, але не досить зрозуміло, хто винний у цьому. Дана інформація, потрапляючи до шахраїв, приносить не тільки моральні, а й матеріальні збитки. Звісно, що за такі дії користувачі і поширювачі конфіденційної інформації про особу повинні нести юридичну відповідальність, зокрема, матеріальну.

Найпоширенішим визначенням інформаційної безпеки є:

Іформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.[1]

Інформаційна загроза діє через публічність: ЗМІ та Інтернет-простір, тим самим маючи вплив на масштабну кількість людей.

В даний час, коли країна переживає тяжкі часи, будь-яка неправдива або спотворена інформація може викликати емоційний вибух серед населення. Передача такої інформації здатна зробити з невинної людини ворога і навпаки. Особливо цьому сприяють, нажаль, ЗМІ. На сьогодні це один з наймасштабніших способів маніпуляції людьми. Вони фактично контролюють наше життя та панують над нашою свідомістю.

Серед ЗМІ варто виділити саме телебачення. В наш час телебачення – це бізнес. Воно нав'язує свою думку, надає нам різноманітну інформацію, яку більшість людей не здатна аналізувати і сприймає як єдино можливу та правдиву. Телеканали не гребують нічим для завоювання аудиторії: чим більша аудиторія, тим більший прибуток вони мають. Все просто, ми дивимось - вони заробляють. Телебачення слугує інформаційною зброєю між владою та пересічним громадянином. Воно є основним каналом зв'язку, передачі інформації, яким користується більша частина населення.

Розважальні шоу, серіали, новини – це лише короткий список, що ми бачимо кожного дня з блакитних екранів. Ні для кого не є таємниця, що в наш час телебачення є не лише засобом передачі інформації, але й зброєю швидкого та масового впливу на громадян. Найперше на що звертаєш увагу - це специфіка каналів розповсюдження будь-якої інформації для населення, мета та методи впливу на глядача.

Глядачі як клас грають значну, а часом й визначальну роль у сучасному політичному процесі. Тому для більшої зацікавленості людей та ширшої аудиторії телеканали використовують так звані психологічні «прив'язки». Тобто способи, так званого, "зворотного зв'язку" в різних формах: дзвінки в студію під час прямого ефіру, вибір по телефону варіантів відповіді на поставлене питання тощо. Тобто це лише один зі способів формування та маніпулювання громадською думкою.

Маніпуляція - вид психологічного впливу, який використовується для прихованого впровадження в психіку жертви цілей, бажань, намірів, відносин або установок маніпулятора, які не збігаються з актуально існуючими потребами жертви. Це, так зване, приховане управління людьми та їх поведінкою. [2]

Існує декілька шляхів маніпулювання:

- спробувати змусити виконати нав'язану їм дію, тобто зломити опір (відкрите управління);
- замаскувати керуючий вплив так, щоб він не викликав заперечення адресата (приховане управління).

Способів маніпулювання багато, але, абсолютно очевидно, що головним є контроль на всіх рівнях над інформаційним апаратом та апаратом формування ідей людини. Маніпуляція - це лише однин зі способів впливу на формування думки особистості. Протистояти цьому надзвичайно важко, необхідно думати, читати, спостерігати, а головне - аналізувати отриману інформацію та робити самостійні висновки.

Отже, інформаційна маніпуляція сама по собі не є абсолютно об'єктивною загрозою, але в контексті з допоміжним методологічним засобом, наприклад ЗМІ, які представляють собою керуючий апарат над формуванням поглядів та уявлень людей воно стало загрозою XXI ст., боротись з якою практично не можливо.

Література

1. Інформаційна безпека [Электронный ресурс] – Режим доступа: https://uk.wikipedia.org/wiki/Інформаційна_безпека
2. Маніпуляція [Электронный ресурс] – Режим доступа: https://uk.wikipedia.org/wiki/Маніпуляція_(психологія)

РОЗГОЛОШЕННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ВИМОГУ ОРГАНУ ДЕРЖАВНОЇ ВЛАДИ

Чікін С. В.
НТУУ «Київський політехнічний інститут»

В Україні, з обмеженнями відповідно до закону «Про інформацію» [2, ч. 4 ст. 21] та Постанови Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» [3], комерційною таємницею може бути «*інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію*» [1, ч. 1 ст. 505]. До комерційної таємниці може відноситись інформація «*технічного, організаційного, комерційного, виробничого та іншого характеру*» [1, ч. 2 ст. 505], тобто така інформація, неправомірне розкриття якої може нанести збитки її володільцю.

Суб'єкту майнових прав інтелектуальної власності належить «*виключне право дозволяти використання комерційної таємниці*» [1, ч. 1 ст. 506] . Але, як і в інших випадках щодо «виключного права інтелектуальної власності», це «виключне право» не є абсолютним.

В статті 424 Цивільного кодексу України [1, ч. 2 ст. 424] зазначено, що «законом можуть бути встановлені винятки та обмеження в майнових правах інтелектуальної власності» і, як наслідок, в «виключності» права дозволяти використання комерційної таємниці.

Законодавство України (див. - табл.) передбачає низку суб'єктів владних повноважень, на вимогу яких володілець комерційної таємниці має її розкрити (надати відомості, дані, документи тощо).

Таблиця

Перелік органів державної влади, які мають право отримувати конфіденційну інформацію від фізичних і юридичних осіб для реалізації своїх повноважень

№ з/п	Орган державної влади	Підстава	Права органів державної влади з одержання інформації
1	Служба безпеки України (СБУ)	П.3 ч. 1 ст. 25 ЗУ[1)] від 25.03.92 №2229-XII «Про Службу безпеки України»	***Одержувати*** *на письмовий запит керівника відповідного органу Служби безпеки України від міністерств, державних комітетів, інших відомств, підприємств,*

			установ, організацій, військових частин, громадян та їх об'єднань ***дані і відомості****, необхідні для забезпечення державної безпеки України, а також* ***користуватись*** *з цією метою* ***службовою документацією*** *і* ***звітністю****.*
2	Органи, що здійснюють оперативно-розшукову діяльність[2)]	П.4 ч. 1 ст. 8 ЗУ від 18.02.92 №2135-XII «Про оперативно-розшукову діяльність»	***Витребувати***, ***збирати*** *і вивчати* ***документи*** *та* ***дані****, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів.*
3	Органи, що ведуть боротьбу з організованою злочинністю	Пп. «б» п. 2 ст. 12 ЗУ від 30.06.93 «3341-XII «Про організаційно-правові основи боротьби з організованою злочинністю»	*На письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю* ***одержувати*** *від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно від форм власності)* ***інформацію*** *і* ***документи*** *про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб. Надається негайно, а якщо це неможливо, то не пізніш як протягом 10 діб.*
4	Міліція	П.17 ч. 1 ст. 11 ЗУ від 20.12.90 №565-XII «Про міліцію»	***Одержувати*** *безперешкодно і безплатно від підприємств, установ і організацій*

			незалежно від форм власності та об'єднань громадян на письмовий запит ***відомості (в тому числі й ті, що становлять комерційну*** *та банківську* ***таємницю)****, необхідні у справах про злочини, що знаходяться у провадженні міліції.*
5	Державна податкова служба України	П.п. 20.1.2, 20.1.30 ст. 20 Податкового кодексу України від 02.12.2010 №2755-VI	*Під час проведення виїзних перевірок* ***отримувати*** *у платників податків (представників платників податків)* ***копії документів*** *(засвідчені підписом платника податків або його посадовою особою та скріплені печаткою (за наявності)), що свідчать про порушення вимог податкового законодавства або іншого законодавства, контроль за дотриманням якого покладено на органи державної податкової служби;* ***Одержувати*** *безоплатно необхідні* ***відомості*** *для ведення Єдиного реєстру податкових накладних, формування інформаційного фонду Державного реєстру фізичних осіб - платників податків від платників податків, а також Національного банку України та його установ - про суми доходів, виплачених фізичним особам, і утриманих з них*

			податків та зборів (обов'язкових платежів), від органів, уповноважених проводити державну реєстрацію суб'єктів, а також видавати ліцензії на провадження видів господарської діяльності, що підлягають ліцензуванню відповідно до закону, - про видачу таких свідоцтв про державну реєстрацію та ліцензій суб'єктам господарської діяльності, від органів внутрішніх справ - про громадян, які прибули на проживання до відповідного населеного пункту чи вибули з нього, від відділів державної реєстрації актів цивільного стану - про фізичних осіб, які померли.
6	Податкова міліція	Ст. 22 ЗУ від 04.12.1990 №509- XII «Про державну податкову службу в Україні»	П.17 ч. 1 ст. 11 ЗУ від 20.12.90 №565-XII «Про міліцію» (див. п.4 цієї табл.). П.п. 20.1.2, 20.1.30 ст. 20 Податкового кодексу України від 02.12.2010 №2755-VI (див. п.5 цієї табл.).
7	Антимонопольний комітет України	Ст. 16 ЗУ від 26.11.93 №3659-XII «Про Антимонопольний комітет України»	*б) при розгляді заяв і справ про порушення законодавства про захист економічної конкуренції, проведенні перевірки та в інших передбачених законом випадках* ***вимагати*** *від суб'єктів господарювання, об'єднань, органів влади,*

			органів місцевого самоврядування, органів адміністративно-господарського управління та контролю, їх посадових осіб і працівників, інших фізичних та юридичних осіб ***інформацію****, в тому числі з обмеженим доступом;* *9) у випадках та порядку, передбачених законом, проводити огляд службових приміщень та транспортних засобів суб'єктів господарювання - юридичних осіб,* ***вилучати*** *або накладати арешт на предмети,* ***документи*** *чи* ***інші носії інформації****, які можуть бути доказами чи джерелом доказів у справі незалежно від їх місцезнаходження;*
8	Органи дізнання та органи попереднього слідства	Ст. 66 Кримінально – процесуального кодексу України від 28.12.1960 №1001-05	***Вимагати*** *від підприємств, установ, організацій, посадових осіб і громадян* ***пред'явлення*** *предметів і* ***документів****, які можуть встановити необхідні в справі фактичні дані; вимагати проведення ревізій,* ***вимагати*** *від банків* ***інформацію****, яка містить банківську таємницю, щодо юридичних та фізичних осіб у порядку та обсязі, встановлених Законом України "Про банки і банківську діяльність". Виконання цих вимог є*

			обов'язковим для всіх громадян, підприємств, установ і організацій
9	Органи прокуратури України	Ст. 8 ЗУ від 05.11.91 №1789-XII «Про прокуратуру»	***Статистична** та **інша інформація** або їх копії, необхідні для здійснення прокурорського нагляду чи розслідування, **видаються** на вимогу прокурора або слідчого безкоштовно.*
10	Державна комісія з цінних паперів та фондового ринку України	Ст. 8 ЗУ від 30.10.96 №448/96-ВР «Про державне регулювання ринку цінних паперів в Україні»	*8) **Здійснювати контроль за** достовірністю і розкриттям **інформації**, що надається емітентами та особами, які здійснюють професійну діяльність на ринку цінних паперів, і саморегулівними організаціями, та її відповідністю встановленим вимогам.* *21) **Вилучати** під час проведення перевірок на строк до трьох робочих днів **документи**, що підтверджують факти порушення актів законодавства про цінні папери.*
11	Розвідувальні органи України [3)]	Ст. 9 ЗУ від 22.03.2001 №2331-III «Про розвідувальні органи України»	***Отримувати** для розвідувальних цілей необхідну **інформацію** від усіх органів державної влади, підприємств, організацій і установ, включаючи банки, незалежно від форми власності, в тому числі інформацію з*

			автоматизованих інформаційних та довідкових систем, банків даних тощо у порядку, визначеному законом.

[1] ЗУ – закон України.

[2] Статтею 5 ЗУ «Про оперативно-розшукову діяльність» передбачено, що оперативно-розшукова діяльність здійснюється оперативними підрозділами МВС, СБУ, Прикордонних військ України, управління державної охорони, оперативними підрозділами податкової міліції, органів і установ Державного департаменту України з питань виконання покарань.

[3] До розвідувальних органів України, відповідно до ст. 6 ЗУ «Про розвідувальні органи України», відносяться: Служба зовнішньої розвідки України, розвідувальний орган Міністерства оборони України та розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону.

Аналіз зазначених в таблиці нормативно-правових актів виявив, що вони здебільшого містять вимоги щодо нерозголошення представниками суб'єктів владних повноважень такої отриманої інформації.

Так, наприклад, відповідно до ст. 35 закону «Про Службу безпеки України» [4] співробітники Служби безпеки України, які виконують свої обов'язки відповідно до наданих законодавством повноважень і в рамках Закону, не несуть відповідальності за завдані майнові збитки. Але відповідно до ч. 1 ст. 19 «Про організаційно-правові основи боротьби з організованою злочинністю» [5] підрозділи органів внутрішніх справ і Служби безпеки України вживають заходів щодо захисту зібраної інформації про події і факти, що свідчать про організовану злочинну діяльність, її причини та умови, про осіб, які беруть участь в організованій злочинній діяльності.

Крім цього, наприклад, відповідно до законів:

«Про Антимонопольний комітет України» [6] (ст. 22-1) за розголошення комерційної таємниці працівники Антимонопольного комітету України, його територіальних відділень несуть відповідальність, встановлену законом.

«Про оперативно-розшукову діяльність» [7] (ст. 9) забороняється оприлюднювати або надавати зібрані відомості, а також інформацію щодо проведення або не проведення стосовно певної особи оперативно-розшукової діяльності до прийняття рішення за результатами такої діяльності.

Однак вимог щодо оформлення запиту або вимоги щодо надання інформації, що становить комерційну таємницю, (наявність печатки, бланку суворої звітності тощо) законодавство не містить.

Література

1. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356.

2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII // Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650.

3. Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. N 611 // Урядовий кур'єр, 1993, N 48.

4. Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII // Відомості Верховної Ради України (ВВР), 1992, N 27, ст.382.

5. Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» від 30.06.1993 № 3341-XII // Відомості Верховної Ради України (ВВР), 1993, N 35, ст.358.

6. Закон України «Про Антимонопольний комітет України» від 26.11.1993 № 3659-XII // Відомості Верховної Ради України (ВВР), 1993, N 50, ст.472.

7. Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135-XII // Відомості Верховної Ради України (ВВР), 1992, N 22, ст.303.

ДЕЯКІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМ

Юдкова К.В.
НДІІП НАПрН України,
НТУУ «КПІ»

Забезпечення безпеки інформації є процесом, нерозривно пов'язаним із забезпеченням безпеки всієї інформаційної системи. При цьому доцільним буде розглядати правові основи забезпечення безпеки саме інформаційно-телекомунікаційних систем, оскільки в цьому випадку базисом правового регулювання є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Таким чином, для цілей цієї роботи термін інформаційні системи та похідні вживаються в значенні інформаційно-телекомунікаційні системи за дефініцією Закону.

Відповідно до ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007, інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [1]. Прикладом ненормативного визначення є така дефініція: інформаційна безпека є процес зберігання інформації в стані захищеності її доступності, цілісності і конфіденційності [2].

Набір імперативів щодо процесу контролю та регламентації порядку доступу суб'єктів до визначених правових ресурсі, порядок аудиту дії користувачів в інформаційній системі, захист комунікаційного потоку тощо формує політику безпеки. В свою чергу, для реалізації того чи іншого типу (або рівня, в залежності від критеріїв класифікації) політики безпеки існують правові, організаційно-адміністративні та інженерно-технічні засоби захисту інформації.

Правове забезпечення інформаційної безпеки – є сукупністю законодавчих актів, нормативно-правових документів, положень, інструкцій, директивних вимог тощо що містять правові норми щодо регулювання діяльності суб'єктів в сфері інформаційної безпеки та, за своєю суттю, є правовим режимом інформаційної безпеки.

Інформаційна безпека є перманентним процесом сталого розвитку, а сама модель інформаційної безпеки, для забезпечення досягнення її основних цілей, обов'язково має бути динамічною та гнучкою, мати можливість розвиватися та здатність до перебудови та зміни власних структурних елементів. Таким чином, правовий режим має ґрунтуватися

саме на можливостях динамічної реакції на подразники у вигляді інформаційних загроз.

Станом захищеності інформацій є такий її стан, коли зберігаються три основні її характеристики:

- о конфіденційність - стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на неї право [3];
- о цілісність - уникнення несанкціонованої модифікації інформації [3];
- о доступність - уникнення тимчасового або постійного приховування інформації від користувачів, що отримали права доступу [3].

Загострення проблем безпеки в світі в цілому поставило питання забезпечення національної, соціальної, організаційної безпеки в тому числі і в інформаційній сфері.

Так, в 1983 р. міністерство оборони США розробило «Помаранчеву книгу» - «Критерії оцінки надійних комп'ютерних систем» ("Trusted Computer System Evaluation Criteria (TCSEC), що стало фактичним початком запровадження системи захисту інформації без фокусування на її підвідомчості. В 1980-1990-х роках схожі документи були опубліковані в деяких країнах Західної Європи, наприклад, Information Technology Security Evaluation Criteria, які пізніше були замінені на Common Criteria for Information Technology Security Evaluation.

В Україні з метою забезпечення захисту інформації в інформаційних системах було прийнято Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та на виконання ст. 10 вказаного Закону також було прийнято Постанову КМ України «Про затвердження Правил забезпечення захисту в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Вказані Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, тобто, фактично, інформації з обмеженим доступом.

Таким чином, єдиного підходу до забезпечення безпеки в інформаційних системах не сформовано. Більше того, якщо дослідити правозастосовну практику на прикладі судових рішень, то можна дійти висновку, що застосуванню підлягали лише ті положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», які пов’язані із застосування комплексної системи захисту інформації з підтвердженою відповідністю. Тобто критична більшість судових рішень з вибірки в 50-60 рішень (2014-2015 р.р.) містили посилання на статтю 8 вказаного закону - «Умови обробки інформації в системі». Деякі судові рішення містять додаткові контекстуальні посилання на термінологічні визначення з огляду на юрисдикцію Закону України «Про авторське право та суміжні права», тобто розглядають інформацію в розрізі захисту прав інтелектуальної власності. Можна вважати, що достатньою мірою врегульованими є питання охорони виключних прав і частково захисту інформації (в рамках державної

таємниці) з огляду на встановлення міри відповідальності особам, винним у порушенні законодавства України про захист інформація.

Окрім вже зазначених особливостей, вищевказаний Закон містить термінологічне визначення володільця інформації - фізична або юридична особа, якій належать права на інформацію [4]. При цьому, нормативного визначення права на інформацію в даному контексті в Україні не існує, оскільки право на інформацію тлумачиться занадто широко як невід'ємне право людини на доступ до інформації.

Таким чином, можна дійти висновку, що правозастосуванню в більшості випадків підлягають тільки норми нормативного акту щодо встановлення відповідальності за вчинені правопорушення. При цьому зберігається термінологічна невизначеність, звуження суб'єктного складу та розмиття предмету регулювання.

Література

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] Юридичний журнал. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222

3. Техническая защита информации: Приказ Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст [Електронний ресурс] – Режим доступу: http://zakon.law7.ru/base09/part0/d09ru0812.htm

4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286

ЗАБОРОНА ЗЛОВЖИВАННЯ ПРАВОМ НА ІНФОРМАЦІЮ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДЕЯКІ ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ

Яременко О.І.
Вінницький державний педагогічний університет

Інформаційний розвиток сучасного суспільства передбачає необхідність правової охорони та захисту не тільки права на інформацію, як одного із ключових інститутів національного права України, а й законодавчого регулювання заборони зловживання цим правом. В першу чергу це обумовлюється тим, що високий рівень соціальної цінності права на інформацію поєднується із значною кількістю загроз для особи, суспільства, держави, які виникають в процесі його реалізації, що актуалізує наукові дослідження в цій сфері.

Метою статті є аналіз поняття «зловживання правом на інформацію» та дослідження окремих теоретичних і практичних проблем законодавчого регулювання заборони зловживання цим суб'єктивним правом.

Незважаючи на доволі тривалу еволюцію поглядів науковців на таке негативне явище правової реальності як зловживання правом, в загальній теорії права воно не знайшло однозначного трактування. Сучасні науковці в основу дефініції цього поняття покладають такі ознаки, як наявність протиріччя між призначенням суб'єктивного права і наслідками його здійснення, недобросовісність, шкідливість. Так, Рєзнікова В.В. пропонує авторське визначення зловживання правом як вольової та усвідомленої діяльності (дії) суб'єкта з недобросовісної реалізації суб'єктивного права не за його призначенням, що заподіює шкоду суспільним інтересам та/або особистим інтересам третіх осіб чи створює реальну загрозу її заподіяння при формальній правомірності такої діяльності її дій [1, 34].

Шипілов Л.М. зловживання правом трактує як особливий вид правової поведінки, який полягає у використанні громадянами своїх прав у недозволений спосіб, що суперечить призначенню права, внаслідок чого завдаються збитки (шкода) окремій особі, суспільству або державі [2, 7].

Хміль М.М. розуміє зловживання правом, як таку форму здійснення права, за допомогою якої заподіюється шкода іншим учасникам суспільних відносин шляхом здійснення права в протиріччі з його цільовим призначенням або здійсненням дій, що виходять за межі наданих законом прав, якщо такі межі й цілі здійснення права встановлені в законі[3,16].

Різні підходи до зловживання правом також спостерігаються і в приватно - та публічно - правових галузевих юридичних науках. Зокрема, Веніславський Ф.В., досліджуючи зловживання правом з позицій науки конституційного права, вважає, що його сутність полягає у використанні права всупереч соціальному призначенню, для досягнення іншої мети ніж

тієї, необхідність досягнення якої передбачав законодавець в процесі формулювання даного виду поведінки [4, 26].

Шишка Р.В., висвітлюючи цивільно – правові аспекти зловживання правом, трактує цей феномен як поведінку (активну чи пасивну) із здійснення права, але з порушенням встановлених меж, місця, способу і форми їх здійснення. При цьому, він підкреслює, що одним із найбільш типових зловживань суб'єктивними цивільними правами є зловживання саме правом на інформацію та іншими немайновими правами [5, 26]. Цілком погоджуючись з такою думкою, підкреслимо, що ця закономірність поширюється на сферу як приватних, так і публічних правовідносин, у зв'язку з комплексною правовою природою права на інформацію. Це обумовлюється специфікою феномену інформації, як нематеріального об'єкта правових відносин та особливостями її обігу в суспільстві, які приховують в собі значні потенційні можливості для зловживання правом на інформацію.

На думку Новицької Н.Б., зловживання правом на свободу слова та інформації є можливим за наявності закріплення в законі суб'єктивного права вільно поширювати інформацію в будь-який спосіб; наявність реальної можливості реалізації цього права, тобто можливість поширити інформацію через ЗМІ; реалізація суб'єктивного права на практиці, коли суб'єкт, поширюючи інформацію, порушує тим самим право інших суб'єктів на безпечний інформаційний простір; нанесення, в процесі реалізації суб'єктом свого права, є шкоди суспільним відносинам; наявність аморального або недоцільного вчинку [6, 64].

Такий підхід до сутнісних ознак зловживання правом на інформацію виглядає цілком обґрунтованим і побудований на традиційному розумінні змісту інформаційних прав, яке передбачає, що в їх основу покладено такі аспекти як поширення і одержання інформації. Саме за таким принципом в Україні і здійснено конституційно – правове закріплення інформаційних прав в ст. 34 Конституції України, яка передбачає право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Водночас, конституційно правові норми гарантують право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір [7]. Майже аналогічне формулювання права на інформацію закріплено в Законі України «Про інформацію», ст. 5 якого надає можливість кожному вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [8].

Отже, виходячи із змісту суб'єктивного права на інформацію, закріпленому в чинному законодавстві, зловживання цим правом може бути при здійсненні таких операцій, як одержання, використання, поширення, зберігання та захист інформації. При цьому, аналіз законодавства в інформаційній сфері свідчить про нормативне закріплення двох підходів до заборони зловживання правом на інформацію.

Перший підхід базується на ст. 28 Закону України «Про інформацію», яка передбачає, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини. Диспозиція цієї інформаційної норми частково кореспондується із диспозицією конституційної норми, згідно з якою здійснення інформаційних прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. При цьому, діяння, які розглядаються як зловживання правом на інформацію, водночас кваліфікуються як злочини і за них передбачені кримінальні санкції. Так, Кримінальний кодекс України містить ряд злочинів, об’єктивна сторона яких проявляються у поширенні інформації в формі публічних закликів, розголошення інформації чи завідомо неправдивих повідомлень. Зокрема, кримінальна відповідальність передбачена за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (п. 2 ст. 109); публічні заклики чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України (п. ст. 110), публічні заклики до вчинення терористичного акту (п. ст. 258); публічні заклики до агресивної війни або до розв'язування воєнного конфлікту (ст. 436); завідомо неправдиве повідомлення про підготовку вибуху, підпалу або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками; розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя) (п. 1 ст. 168); розголошення відомостей, що становлять державну таємницю (ст. 328) тощо [9].

Таким чином, в рамках першого підходу, зловживання правом на інформацію закріплено в прямому зв’язку із такими категоріями, як законні обмеження права на інформацію та правопорушення. При цьому, наявність ознаки протиправності у діяннях, які кваліфікуються як зловживання правом, дає підстави для критики такого підходу. Так, якщо особа в своїй поведінці вийшла за межі наданого їй суб’єктивного права, то її не можна вважати особою, що здійснила своє право. У цьому випадку вона не зловживає правом, а діє протиправно [10, 24].

Другий підхід базується на нормах ст. 5 Закону України «Про інформацію», яка закріплює правило, згідно з яким, реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. Тобто, в даному випадку під зловживання правом на інформацію розуміється нанесення шкоди

фізичним та юридичним особам в процесі реалізації суб'єктивного права на інформацію при формальному дотриманні правових норм або із латентною протиправністю діяння. Особливістю такого підходу є те, що особу, яка зловживає правом на інформацію, як правило, не можна притягнути до юридичної відповідальності. Одним з таких прикладів, є зловживання правом на доступ до інформації в Рівненській області, де громадянин надіслав до Дубенської райдержадміністрації 300 запитів на публічну інформацію. Це паралізувало роботу структурного підрозділу, який готує відповіді. Запити, зокрема, передбачали надання інформації щодо кількості безпритульних тварин, що знаходяться на території Дубенського району; поголів'я овець у Дубенському районі з 1991-2012 роки по роках; обсяги роздрібного товарообігу у районі поквартально в кожному з років за період з 1991-2012 роки [11].

Іншим прикладом зловживання правом на інформацію, в рамках другого підходу, є поширення відомостей, зміст яких суперечить презумпції добропорядності і наносить шкоду репутації або правам громадян чи юридичних осіб. Так, згідно із статтею 278 Цивільного кодексу України, забороняється поширювати інформацію, якою порушуються особисті немайнові права [12]. На нашу думку, в цьому випадку зловживання правом на поширення інформації носить спірний характер і потребує додаткової правової оцінки, як правило, органами судової влади. Так, відповідно до п.15 Постанови Пленуму Верховного Суду України від 27.02.2009 р. № 1 "Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи" при розгляді справ зазначеної категорії суди повинні мати на увазі, що юридичним складом правопорушення, наявність якого може бути підставою для задоволення позову, є сукупність таких обставин: а) поширення інформації, тобто доведення її до відома хоча б одній особі у будь-який спосіб; б) поширена інформація стосується певної фізичної чи юридичної особи, тобто позивача; в) поширення недостовірної інформації, тобто такої, яка не відповідає дійсності; г) поширення інформації, що порушує особисті немайнові права, тобто або завдає шкоди відповідним особистим немайновим благам, або перешкоджає особі повно і своєчасно здійснювати своє особисте немайнове право [13].

Таким чином, в законодавстві України, заборона зловживання правом на інформацію закріплюється в широкому і вузькому розумінні. В першому випадку воно розглядається з точки зору законного обмеження права на інформацію і кваліфікується як протиправне, винне, шкідливе діяння в інформаційній сфері, за яке передбачена юридична відповідальність, що ототожнює його із правопорушенням. В основу вузького розуміння покладено наявність шкоди правам чи інтересам інших осіб, при здійсненні права на інформацію, за відсутності чи спірності порушення правових норм.

Література

1. Рєзнікова В. В. Зловживання правом: поняття та ознаки / В. В. Рєзнікова // Університетські наукові записки, 2013. – № 1. – С. 23-35.

2. Шипілов Л.М. До питання про поняття та сутність зловживання правом / Л. М. Шипілов // Право і безпека, 2010. – № 1. – С. 6-9.

3. Хміль М.М. Принцип неприпустимості зловживання правом (теоретико-правові аспекти). Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук за спеціальністю12.00.01 — теорія та історія держави і права; історія правових і політичних вчень. — Національний університет внутрішніх справ, Харків, 2005 р.

4. Веніславський Ф.В. Зловживання правом в публічно-правовій сфері як загроза стабільності конституційного ладу України / Ф. В. Веніславський // Університетські наукові записки, 2009. – № 3. – С. 24-29.

5. Шишка Р.Б. Проблема зловживання правом в сучасному цивільному праві / Р. Б. Шишка // Приватне право і підприємництво, 2014. – Вип. 13. – С. 24-27.

6. Новицька Н.Б. Правові аспекти зловживання правом на свободу слова та інформації / Н. Б. Новицька // Науковий вісник Національного університету державної податкової служби України (економіка, право). – 2013. – № 4. – С. 60-66.

7. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.

8. Про внесення змін до Закону України "Про інформацію": Закон України від 13.01.2011р № 2938-VI // Відомості Верховної Ради України . – 2011. – № 32. – ст.313.

9. Кримінальний кодекс України від 05.04.2001 № 2341-III // Офіційний вісник України. – 2001. – № 21.

10. Рєзнікова В. В. Зловживання правом: поняття та ознаки / В. В. Рєзнікова // Університетські наукові записки. - 2013. - № 1. - С. 23-35.

11. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України. – 2003. – № 40-44. – Ст. 356.

12. Іванеско Д. Перший факт свідомого зловживання правом на свободу інформації/ Д. Іванеско [Електронний ресурс]. – Режим доступу: http://blogs.pravda.com.ua/authors/ivanesko/503b959f2432a/.

13. "Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанови Пленуму Верховного Суду України № 1 від 27.02.2009 р. [Електронний ресурс]. – Режим доступу http://zakon4.rada.gov.ua/laws/show/v_001700-09.

СОДЕРЖАНИЕ

Национальная академия наук Украины
Институт проблем регистрации информации

Национальная академия правовых наук Украины
Научно-исследовательский институт информатики и права

Национальный технический университет Украины «КПИ»
Учебно-научный центр информационного права и правовых вопросов информационных технологий ФСП

Информационные технологии и безопасность

Материалы конференции

Выпуск 15

Подписано к печати 13.10.2015. Тираж 100 экз.
Заказ № 812/а. ООО “Инжиниринг”