преступного поведения). – М.: «Проспект», 2007. - 176 с. **63.** *Кудрявцев В. Н. Противоправное бездействие и причинная связь// Советское государство и право. – 1967, № 5. – С. 31.* **64.** *Гринберг М. С. Место преступной небрежности в ряду возмущающих явлений (помех) // Проблемы борьбы с преступной неосторожностью / Научн. ред. П. С. Дагель. – Владивосток: ДВГУ, 1978. – с. 31-39.* **65.** *Гринберг М. С. Субъективный критерий неосторожности и проблемы причинной связи // Актуальные правовые вопросы борьбы с преступностью: Сб. ст. – Томск: Изд-во Томск. ун-та, 1988. – С. 16-22.* **66.** *Тер-Акопов А. А. Преступление и проблемы нефизической причинности в уголовном праве. – М.: «ЮРКНИГА». – 480 с.* **67.** *Шарапов Р. Д. Физическое насилие в уголовном праве. – СПб: Юрид. центр Пресс, 2001. – 298 с.* **68.** *Шарапов Р. Д. К вопросу о бездействии в уголовном праве// Правоведение. - 1998, № 3. – С.100-102.* **69.** *Шарапов Р. Д. Психический вред как последствие девиантного поведения в уголовном праве // Девиантология в России: история и современность. Сборник тезисов докладов и сообщений на Всероссийской научно-практической конференции, г. Тюмень, 21-22 октября 2003. Г. – Тюмень: Изд-во Тюмен.юрид.ин-та МВД РФ, 2003. – С. 32-33.* **70.** *Ярмиш Н. Проблема інформаційної причинності у науці кримінального права // Право України. – 2003, № 7. – С. 119-121.* **71.** *Гродзинський М. М. Улики в советском уголовном процессе. — Ученые труды ВИЮН, вып. VII. М., 1944, с. 79.* **72.** *Строгович М. С. Материальная истина и судебные доказательства в советском уголовном про-цессе. М., 1955. - с. 351.* **73.** *Эйсман А. А. О формах связи косвенных доказательств. - Вопросы криминалистики. - 1964, № 11. - С. 15.* **74.** *Белкин Р. С. Курс криминалистики. В 3 т. – М.: Юристї, 1997 (т.2) – С. 393-403.* **75.** *Герцензон А. А. Введение в советскую криминологию. - М., 1965. - С. 23.* **76.** *Курс советской криминологии: Предмет. Методология. Преступность и ее причины. Преступник.— М.: Юрид. лит., 1985.— 416 с.* **77.** *Минин А. Я. Информатизация криминологических исследований: (теория и методология).— Екатеринбург: Изд-во Урал, ун-та, 1992. – 136 с.* **78.** *Вовченко В. Н. Духовная экоэтика в мире сознания и в Интернете // Сознание и физическая реальность. Т. 2. № 4. 1997. С. 1-14.* **79.** *Pattee, Howard H. Cell psychology: an evolutionary approach to the symbol-matter problem. In: Cognition and Brain Theory Vol. 5, no. 4, 1982, pp. 325-341.* **80.** *Казначеев В. П., Акулов А. И., Кисельников А. А., Мингазов И. Ф. Выживаниенаселения России. Проблемы «Сфинкса XXI века». Новосибирск: Изд-во Новосибирского университета, 2000. – 231 с.* **81.** *Grasse,P.P. Lareconstructiondunidetlescoordinationsinter-indioviduelleschezBellicositemesnatalensisetCubitermessp. La theorie de la stigmergie: Essai d'interpretation des termites constructeurs.- InsectesSociaux, 6, 1959, pp. 41-83.* **82.** *Джонс М. Т. Программирование искусственного интеллекта в приложениях. – М.:ДМК Пресс, 2004. - 312 с.* **83.** *Quastler H. The emergence of biological organization. New Heaven andLondon: Yale University Press, 1964. / Кастлер Г. Возникновение биологической организации. - М.: Мир, 1967. – 92 с.* **84.** *Колупав А. Г., Чернавский Д. С. Перемешивающий слой. // Кратки сообщения по физике.– 1997.– №1-2.– С.12–18.* **85.** *Курдюмов С. П., Малинецкий Г. Г. Нелинейная динамика и проблемы прогноза // Вестник Российской академии наук, т. 71, № 3, 2001. – С. 210-232.* **86.** *Костенко О. М., Культура і закон - у протидії злу: Монографія. – К.: Атіка, 2008. – 352 с.*

УДК 354:007

ВПЛИВ ВІРТУАЛЬНИХ СПІЛЬНОТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ: СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ

Ігор Гриненко, Дарія Прокоф'єва-Янчиленко*

*Національна Академія Служби безпеки України, *Служба безпеки України*

Анотація: **Розглядаються проблеми, пов'язані із впливом віртуальних спільнот на національну та міжнародну безпеку.**

Summary: **The article deals with the issues of influence, posed by virtual communities on national and international security.**

Ключові слова: **Інформаційна сфера, інформаційна безпека, віртуальні спільноти, «хактивізм»**

І Вступ

Інформаційна революція зумовлює появу нових викликів у сфері політики, культури, економіки та національної безпеки. Прогрес комунікаційних систем, нові методи зберігання інформації вимагають приділення додаткової уваги таким питанням, як захист персональних даних, національний суверенітет та безпека суспільства. Ці зміни також зумовлюють нові погляди на національну безпеку та вимагають інноваційного реагування на сучасні загрози. На міжнародній арені з'являються нові актори – віртуальні об'єднання, що досить швидко набувають можливості суттєво впливати на сферу національної та

міжнародної безпеки. Це може призвести до нового класу міжнародних конфліктів між цими групами та національними державами, або конфліктів між суто віртуальними суб'єктами.

Дослідження впливу таких віртуальних об'єднань на інформаційний простір є важливою передумовою напрацювання заходів із забезпечення національної та міжнародної безпеки як у інформаційній, так і в інших сферах життєдіяльності суспільства.

Сучасні дослідження інформаційної безпеки стосуються переважно технічних питань захисту інформації, що знаходиться в комп'ютерних системах. Вплив різного роду неформальних об'єднань, сформованих з використанням сучасних інформаційних технологій, також найчастіше розглядається через призму захисту даних – питанням функціонування таких об'єднань, їх сучасної та потенційної ролі в суспільному житті приділяється значно менша увага.

Правовому регулюванню інформаційних відносин приділялася увага в роботах вітчизняних та зарубіжних вчених: Є. Макаренка, А. Марущака, Є. Скулиша, В. Цимбалюка, І. Бачила, Б. Губермана, Я. Лойда та інших. Суттєва увага дослідників приділялася також питанням протидії інформаційному впливу з боку державних акторів. Зокрема, маються на увазі дослідження О. Бєлова, В. Горбуліна, С. Зелинського, С. Кара-Мурзи, Г. Почепцова, М. Маклуена, С. Расторгуєва, Е. Армістеда, В Швартау та Е Уолтса.

Однак у таких дослідженнях питанням впливу на інформаційну безпеку з боку віртуальних об'єднань достатня увага не приділялася, зокрема і через те, що такого роду об'єднання є відносно новим феноменом.

З огляду на це, метою статті є розкриття сутності віртуальних об'єднань та їх впливу на інформаційну безпеку на національному та міжнародному рівнях. Для досягнення цієї мети мають бути виконані такі завдання: визначення сучасних тенденцій в інформаційному просторі, що обумовлюють існування віртуальних об'єднань, ступінь їх впливу на інформаційну безпеку та можливостей подальшого розвитку такого впливу.

II Результати досліджень

Однією із найбільш фундаментальних характеристик інформаційної епохи стала зміна самої ідеї зв'язку. Основним інструментом при цьому є глобальна інформаційна мережа Інтернет, обсяги інформації у якій подвоюються щороку. Зростає значення зв'язку між державними структурами, елементами національної інфраструктури, телекомунікаційними, фінансовими, транспортними та аварійними службами. Навіть у тих випадках, коли інформація не передається безпосередньо через мережу Інтернет, для її передачі часто використовуються ті самі фізичні канали.

Процеси інформатизації, звісно, надають нові можливості та переваги, однак залежність від інформаційних технологій робить держави та суспільні утворення більш вразливими для таких атак, як втручання у роботу комп'ютерних систем, розповсюдження комп'ютерних вірусів, проникнення через мережеві екрани чи напади кібертерористів. Як інформаційне середовище, Інтернет за своєю природою є місцем із підвищеним ступенем небезпеки, оскільки є децентралізованою системою, що забезпечує певну анонімність користувачів. Можливості встановлення зловмисників є досить обмеженими, так само, як і можливості запобігання зловживанню ними відкритістю ресурсів. У цьому контексті ключовою дилемою національної безпеки в інформаційну еру стає створення ефективних та прозорих систем управління, які, в той же час, були б здатними захистити громадян та життєво важливі національні інтереси. З одного боку, обмін інформацією посилює ризик з точки зору безпеки, але з іншого – відмова від такого обміну звужує можливості систем управління.

Комп'ютерні технології належать до критичних інфраструктур, захист яких потребує посиленої уваги. Вони є важливими не лише як інструмент для забезпечення функціонування таких інфраструктур, як транспорт чи енергетика, а й самі по собі мають стратегічне значення.

Як свідчать матеріали розслідувань терористичних атак 11 вересня 2001 року, однією із причин цієї трагедії була неадекватність системи інформаційного обміну між різними відомствами Сполучених Штатів – ФБР не реалізувала оперативні дані щодо членів Аль-Кайди, які, як з'ясувалося у подальшому, були одними з організаторів терактів. З огляду на це, керівництвом країни було прийнято рішення щодо розширення обміну конфіденційною інформацією з метою посилення оперативної ефективності систем забезпечення національної безпеки. Урядом США була впроваджена нова політика інформаційного обміну, реалізація якої була покладена на низку відомств, у тому числі Міністерство оборони та Державний департамент.

Результатом стало суттєве збільшення кола осіб, що отримали доступ до конфіденційної інформації. На сьогодні в США доступ до інформації із найвищим рівнем конфіденційності мають 854 тисячі осіб. Останні десять років дипломатична інформація передавалася через мережу SIPRNet (Secret Internet Protocol Router Network), функціонування якої забезпечувалося Міністерством оборони. Доступ до цієї мережі мали співробітники Міністерства оборони та Державного департаменту в усіх країнах світу – всього декілька мільйонів осіб. Система контролю за доступом до цієї мережі не була запрограмована на ідентифікацію

неавторизованих спроб завантажити дані будь-ким, хто мав доступ до інформаційного пулу. Розробники системи в забезпеченні її безпеки покладалися на її користувачів. Результатом цього став витік інформації, яка пізніше була опублікована на сайті WikiLeaks – всього 77 тисяч документів щодо війни в Афганістані, майже 400 тисяч документів щодо війни в Іраку та близько 250 тисяч документів дипломатичного листування з оцінками терористичної загрози, діяльності світових лідерів тощо. За результатами розслідування встановлено, що усі ці документи були завантажені однією особою – рядовим військовослужбовцем з одного комп'ютера. Ця подія стала суттєвою віхою у зміні парадигми інформаційної безпеки, що вказала на уразливість існуючих систем захисту даних зокрема та сучасного суспільства в цілому для загроз у інформаційній сфері [1].

Таким чином, інформаційна ера сформувала середовище, у якому держава та суспільство стали вразливішими, оскільки інформація вже зберігається не в сейфі, надійно закритому від сторонніх очей, а в віртуальному просторі, доступ до якого відкритий з будь-якої точки земної кулі. Загроза інформаційній безпеці може полягати як у оприлюдненні конфіденційних даних, так і в їх руйнації. Протидія таким загрозам пов'язана і з їх транснаціональним характером – на конвенційному рівні ці питання залишаються до цього часу неузгодженими.

Віртуальний простір розглядається військовими як потенційний театр військових дій – сьогодні більше 20% військового бюджету США витрачається на заходи, пов'язані із кіберсектором. У той же час, військовий сектор відчуває загрози з боку віртуального простору – так, комп'ютерна система Пентагону щодня зазнає до шести мільйонів спроб несанкціонованого втручання.

Іншою ознакою останнього часу став феномен віртуальних спільнот транснаціонального характеру, діяльність більшості з яких має нейтральний або суспільно-корисний характер, проте окремі прояви їхньої діяльності можуть характеризуватися як такі, що становлять загрозу національній та міжнародній безпеці. Віртуальні спільноти, що діють у режимі он-лайн, створюють нові можливості для громадянського суспільства, але також мають і значний потенціал у вчиненні асиметричних атак. Інтернет є ефективним інструментом для проявлення соціальної та політичної активності, може бути корисним як індивідуумам та невеликим групам із обмеженими ресурсами, так і великим, добре профінансованим організаціям та коаліціям. Він полегшує залучення прибічників, формування транснаціональних спільнот та коаліцій, дозволяє координувати дії на регіональному та міжнародному рівнях.

Так, сьогодні соціальна мережа Facebook об'єднує людей більше, аніж їх проживає у будь-якій країні світу, окрім хіба що Китаю та Індії (зокрема, очікується, що в 2012 році кількість користувачів Facebook перевищить 1 мільярд осіб). Ця та подібні до неї соціальні мережі відіграє ключову роль в забезпеченні організаційного зв'язку між учасниками різного роду громадських акцій, використовується для напрацювання ідеологічних підґрунть, обміну матеріалами та практичними порадами. Соціальні мережі стають також організаційною площадкою груп так званих «хактивістів», що узгоджують там питання проведення своїх акцій.

Феномен «хактивізму», тісно пов'язаний з існуванням такого роду віртуальних об'єднань, є відносно новою формою соціального протесту та висловлювання ідеології шляхом використання хакерських технік, пов'язаних із втручанням у роботу комп'ютерних систем. Комп'ютерні атаки здійснюються хактивістами скоріше з метою декларування власних ідей, аніж вчинення корисливих злочинів. Вперше подібні атаки були зафіксовані у 1989 році, але значного поширення вони набули лише останнім часом.

Явище «хактивізму» обумовлено двома зустрічними тенденціями – політизацією хакерів та «залученням до Інтернету» активістів рухів соціального протесту, що намагаються перенести акції громадської непокори до віртуального простору. Замість традиційних форм – перекриття магістралей, блокування урядових закладів, приміщень корпорацій блокується робота електронних ресурсів таких установ шляхом несанкціонованого втручання, як правило через мережу Інтернет. Звичайно, не слід перебільшувати роль соціальних мереж у громадських діях – вони можуть лише забезпечувати інформаційний обмін та надавати можливості для координації дій, а не ініціювати соціальні процеси.

Використання громадськими об'єднаннями мережі Інтернет можна поділити на три категорії:

громадська активність – суспільно-прийнятне використання мережі для висловлення політичних поглядів, включає пошук та отримання інформації, створення сайтів, розміщення електронних публікацій, обговорення проблем, створення громадських об'єднань та координації їх діяльності;

«хактивізм» - поєднання активності та хакерства, що включає дії, спрямовані на порушення нормальної роботи ділянок мережі, без завдання серйозної шкоди; блокування доступу до електронних ресурсів без руйнації останніх;

кібертероризм – терористичні дії у кіберпросторі, який охоплює політично-мотивовані хакерські дії, що вчиняються з метою завдання суттєвої шкоди життю людини чи суспільства [2].

Ступінь шкоди збільшується від категорії до категорії, що може і не означати більшого політичного впливу – так, електронний заклик з мільйоном підписів може мати більший вплив, аніж кібер-напад, що перериває нормальну роботу якоїсь державної служби.

Звичайно, різниця між хактивізмом та кібертероризмом є досить умовною і часто залежить від конкретних обставин та суб'єктивної оцінки події [3].

Найвідоміша група хактивістів – Anonymous – раніше проводила кампанії проти Ірану, Австралії та церкви саєнтології, але її активність значно зросла після згаданої публікації матеріалів WikiLeaks у 2010 році. У своєму «маніфесті» Anonymous оголосили початок «інформаційної війни» і як перший об'єкт атаки визначили платіжну систему PayPal. Після цього кібератак зазнали сайти не лише PayPal, а й Mastercard, Visa та інших компаній, які припинили обслуговування WikiLeaks, тобто переведення на користь останніх фінансових пожертвувань. Об'єктами атаки також став швейцарський банк PostFinance, який закрив рахунок Джуліана Ассанжа, та прокуратура Швеції.

Anonymous є скоріше ідеологією, аніж стійкою групою людей. Послідовники цієї ідеології виступають за загальнодоступність інформації та борються проти утискання свобод урядами та корпораціями, проти корупції та інших негативних проявів суспільного життя, які частина цієї спільноти не схвалює. Anonymous не має лідерів та уповноважених представників, так само як і будь-якої усталеної структури. «Членство» у «групі» проявляється через участь у її операціях, при цьому функції переважної більшості учасників є вкрай простими. Правилом для учасників є залишатися анонімним та захищати анонімність інших. Фактично, оголосити операцією Anonymous можна будь-яку кібер-атаку, причому зробити це також може будь-хто. Деякі операції не підтримуються більшістю – наприклад, окремі спроби викрасти та опублікувати особисту інформацію громадян, але вони, тим не менш, декларуються від імені групи.

Група Anonymous за останні роки значно розширилася, стала більш скоординованою і має достатньо ресурсів для завдання шкоди урядовим та корпоративним системам. Сьогодні з цією групою асоціює себе декілька сотень тисяч осіб.

З огляду на зростання активності Anonymous зокрема та інтернет-спільнот взагалі, останнім часом вони стали об'єктом інтересу не лише правоохоронних та інших державних структур окремих країн, а й міжнародних організацій. Так, діяльність цієї групи розглядалася у звіті лорда Джопліна в Парламентській асамблеї НАТО в червні 2011 року «Інформація та національна безпека». У звіті, зокрема, вказувалося на те, що дилема між прозорістю та конфіденційністю стала однією із ознак інформаційної ери. Навіть за найвищої відкритості державного управління, військові та розвідувальні операції не можуть плануватися та здійснюватися без дотримання певного рівня конфіденційності. За словами доповідача, «прозорість не може існувати без контролю». Уряди, передусім у особі структур сектору безпеки, повинні мати право обмежувати доступ до інформації з метою забезпечення належного управління та захисту. Уряди та корпорації мають ті самі права на забезпечення секретності власних даних, що і громадяни, і забезпечення певного рівня конфіденційності є необхідним для ефективного управляння державними інституціями та організаціями. Окрім цього, у низці випадків прозорість може бути предметом зловживання – як через непрофесійну та завідомо неправильну інтерпретацію інформації та документів, так і шляхом упередженого аналізу, через нестачу досвіду тощо. Тому не все, що носить ярлик «прозорості» є корисним для уряду та людей. Більше того, невиправдана «прозорість» призводить до того, що політичні процеси стануть більш закритими – зникне відвертість у спілкуванні між дипломатами, що сьогодні дозволяє вирішувати питання міжнародного порядку денного поза межами офіційних акцій. Це також збільшить тиск на осіб, що приймають рішення, дії яких відразу ж стануть відомими як громадянам, так і урядам інших держав. Такий тиск є не тільки непотрібним, а й загрозливим, передусім у секторі безпеки [1].

Зазначена доповідь містила досить ґрунтовний аналіз актуальних загроз у інформаційній сфері. З іншого боку, окремі тези цієї доповіді можуть бути витлумачені таким чином, що ніби-то інтереси держави та народу в інформаційній сфері можуть суперечити одне одному. Окрім цього, визначення права урядів та корпорацій на конфіденційність інформації, хоча само по собі є повністю виправданим та логічним, висловлене як абсолютне, також має досить контроверсійний характер – адже будь-які права юридичних осіб та держав є похідними від прав громадян чи осіб, яких вони представляють. Права корпорацій є похідними від законних прав їх акціонерів так само, як і права держав є похідними від прав громадян, що є їх «акціонерами», довіряючи їм вираження та забезпечення своїх інтересів. На ці суперечливі моменти і була звернута увага активістів Anonymous у відповіді на цей звіт.

Окремі дії групи Anonymous мають соціально-корисний характер, зокрема, спроба, хоча і не доведена до кінця, вплинути на діяльність мексиканського наркокартелю Los Zetas восени 2011 року [4 – 6], а також ліквідація шляхом цілеспрямованих «хакерських актак» мережі сайтів, що займалися розповсюдженням дитячої порнографії [7].

Водночас, не всі прояви громадянської активності групи можна оцінити як позитивні. Так, нещодавно Anonymous оприлюднили імена та адреси декілька сотень співробітників поліції Техасу, чим поставила під загрозу життя цих правоохоронців та їх родин. Ці дії активісти групи пояснювали тим, що щодо співробітника поліції, звинуваченого у причетності до розповсюдження дитячої порнографії, не було обрано запобіжного заходу у вигляді взяття під варту. Фактичною ж причиною було закриття одного із сайтів Anonymous. На початку лютого 2012 року ФБР США визнало, що Anonymous змогла підключитися до міжнародної правоохоронної відео-конференції, на якій розглядалася загроза з боку цієї групи та відкрила доступ до цього відео через Інтернет [8].

В цілому можна вважати зазначені механізми впливу таких віртуальних спільнот «інформаційною зброєю» нового покоління, яка дозволяє суттєво впливати на розвиток подій у глобальному масштабі. Поява зазначеної «віртуально-соціальної технології» докорінно змінить баланс сил не тільки в інформаційному, але й у фізичному просторі, при чому не тільки і не стільки збитками, що можуть бути завдані, скільки самою потенційною можливістю настання таких збитків. Вплив цих технологій має і буде враховуватися всіма акторами – політичними, економічними, тощо. Тенденції суспільного розвитку, обумовлені прогресом інформаційних технологій, дозволяють передбачити, що такі транснаціональні віртуальні спільноти вже в найближчому майбутньому можуть стати могутнішими не лише за традиційні легальні та нелегальні комерційні структури, а й за деякі державні утворення.

Розвиток інформаційних технологій не лише зумовлює перехід характеру економічної та культурної революції на якісно новий рівень, але й призводить до якісного розвитку зворотного зв'язку між індивідуумом та суспільством та між суспільством та державою. Обсяг свободи індивідуума, сфера його діяльності будуть постійно розширюватися. При цьому Інтернет поступово перетворюється на колективний розум та волю людства (ця тенденція вже тривалий час привертає увагу науковців – зокрема, слід з цього приводу відзначити міжнародний проект "Brain Web", що має на меті перетворення Інтернету на справжній розподілений інтелект з використанням принципів бутстрапу [9 – 10]) .

Інтернет-спільноти, діючі як колективний розум, мобілізуватимуть суспільство, поповнюючи таким чином свої ряди, що в кінцевому рахунку зробить їх діяльність більш соціально-прийнятною, менш радикальною щодо держав та інших легальних суб'єктів. Таким чином, процеси глобалізації вийдуть на принципово новий рівень – формування можливостей спілкування та впливу в глобальному масштабі, на умовах, більш прийнятних для людства в цілому. Нові технології принципово змінюють поняття влади, роблячи її доступнішою для суспільства, підзвітною та підконтрольною останньому. Вплив інформаційних технологій призводить до формування принципово нового суб'єкта політики, що діятиме в глобальному масштабі на принципах прямої демократії та меритократії. З іншого боку, індивідууми, позбавлені з об'єктивних чи суб'єктивних причин можливостей користуватися такими технологіями, будуть обмежені в можливостях впливу на суспільні процеси, тобто фактично зазнають обмеження своїх законних прав.

Аналізуючи розвиток інтернет-спільнот, можна виділити низку основних тенденцій. По-перше, це сегментація спільнот, виділення своєрідної «еліти» за принципом кращого володіння інформаційними технологіями, що виконує окремі акції якісно іншого рівня, які вимагають більш професійного підходу. В принципі, формування технократичних еліт передбачалося вже десятиріччя тому, тож цілком ймовірно, що сучасні процеси відбуваються саме у рамках такого напряму.

Можливим є як створення нових підгруп у складі вже наявних інтернет-спільнот, так і включення до останніх вже усталених хакерських груп, які при цьому якісно змінюватимуть масштаби та характер своєї діяльності. Окремі з них, наприклад, «Народний визвольний фронт» (Peoples Liberation Front (PLF)) існують вже з 1985 року, інші, такі як AnonOps є відносно новими із сформувалися вже у складі Anonymous. Незважаючи на те, що ядра таких підгруп є відносно невеликими, при проведенні своїх акцій вони можуть розраховувати на фактично необмежені ресурси глобальної хактивістської спільноти. Такі групи, як правило, є більш централізованими і проявляють активність лише у окремих випадках, що отримують значний суспільний резонанс, наприклад у атаках на веб-сайти урядових структур Тунісу, Ірану, Єгипту та Бахрейну в 2010 – 2011 роках. Членство у таких підгрупах є обмеженим – як правило, лише за відповідними запрошеннями («інвайтами»).

Окрім цього, відбувається сегментація спільнот за територіальною ознакою, з метою вирішення місцевих питань. Із розширенням та удосконаленням арсеналу таких спільнот зростатиме і їх ефективність, можливості вирішувати питання навіть без застосування своїх реальних можливостей.

Водночас, головним механізмом еволюції надалі буде не групова або індивідуальна селекція, а так зване бутстрапування, або ж мережева селекція (network selection), як еволюція корпоративної мережі, що здатна до самоорганізації [11].

В цілому ж технологічний прогрес, як і будь-яке суспільне явище, несе в собі як позитивні наслідки, так і загрози. Так само і розвиток Інтернет-спільнот, що є неминучим етапом інформаційного розвитку, несе у

собі не тільки позитивні риси, а й потенційні та вже реальні загрози. Усунення цих загроз традиційними методами навряд чи є скільки-небудь можливим і вимагає нових системних підходів, адаптації усієї системи державного управління до нової суспільної ситуації.

III Висновки

Узагальнюючи викладене, можна зробити висновки про те, що існування віртуальних спільнот, побудованих шляхом використання сучасних телекомунікаційних технологій є суттєвим чинником, що впливає на національну та міжнародну безпеку. Формування таких спільнот обумовлено як розширенням інформаційної сфери, залученням до неї традиційних акторів, так і диверсифікацією активності в рамках кіберпростору. Діяльність зазначених віртуальних акторів має виражений транснаціональний характер і, з одного боку, виражає певні законні інтереси громадськості, а з іншого – несе у собі певні загрози та виклики, що мають враховуватися при напрацюванні систем та заходів забезпечення інформаційної безпеки. З іншого боку, можна передбачити розширення сфери впливу таких структур, що відіграватимуть все більшу роль у формуванні не лише інформаційного середовища, а й широкому спектрі процесів суспільного життя.

Література: ***1.*** *Jopling. Information and National Security.171 CDS 11 E: Draft General Report. General Rapporteur: (United Kingdom). – 01. 06. 2011 [Електронний ресурс]. Режим доступу: http://www.nato-pa.int.* ***2.*** *Denning E. D. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University [Електронний ресурс]. Режим доступу: http://www.iwar.org.uk/ cyberterror/resources/denning.htm.* ***3.*** *Arquilla J., Ronfeldt D. Networks and Netwars. The Future of Terror, Crime, and Militancy. – 2001 [Електронний ресурс]. Режим доступу: www.rand.org.* ***4.*** *Norton Q. Anonymous Skeptical of Proposed Attack on Zetas Drug Cartel. – October 31, 2011 [Електронний ресурс]. Режим доступу: www.wired.com.* ***5.*** *Mexico: Video threatens to disclose Zetas allies : Associated Press – 31.10.2011 [Електронний ресурс]. Режим доступу: www.ap.org.* ***6.*** *John P. M. Jr. Anonymous Takes On Mexican Drug Cartel : PCWorld. – 30. 10. 2011 [Електронний ресурс]. Режим доступу: www.pcworld.com.* ***7.*** *Anonymous: Борьба с детской порнографией – 09. 11. 2011 [Електронний ресурс]. Режим доступу: http://it-sektor.ru.* ***8.*** *Shane S. F.B.I. Admits Hacker Group's Eavesdropping. – 03. 02. 2012 [Електронний ресурс]. Режим доступу: http://www.nytimes.com.* ***9.*** *Heylighen, F. & Bollen J. The World-Wide Web as a Super – Brain: from metafor to model, in: Cybernetics and Systems 96, R. Trappl (ed.), (Austrian Society for Cybernetics, 1996, p. 917–922.* ***10.*** *Heylighen, F . Bootstrapping knowledge representations: from entailment meshes via semantic nets to learning webs. – International Journal of Human-Computer Studies, 1997.* ***11.*** *Казанський А. Б. Модели организационно замкнутых систем и контуры развития новых подходов в области искусственного интеллекта и когнитивной науки [Електронний ресурс]. Режим доступу: spkurdyumov.narod.ru/kazanskiy.html*

УДК 621.391

МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ В ОРГАНИЗАЦИЯХ, ИСПОЛЬЗУЮЩИХ СВЕДЕНИЯ, СОДЕРЖАЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

Давуд Рустамов, Мирза Рзаев
Министерство Национальной Безопасности Азербайджанской Республики

Анотація: **Запропонована модель забезпечення безпеки реляційних баз даних (РБД) відомостей, що містять державну таємницю. Такі типи баз потребують особливого підходу до забезпечення їх безпеки. Рішення питання про визначення грифа секретності документів, тобто розподіл інформації за категоріями конфіденційності, а також розподіл користувачів на групи з різними рівнями доступу і обмеженнями в доступі до електронних документів, що визначається структурою організації і штатною структурою подрозділів (начальники, заступники, рядові службовці, і т. п.), свідчать про актуальність методики, що запропонована авторами.**

Summary: **Offered model of providing of safety of relyaciynikh bases of these (RBD) information, that mistyat'derzhavnu secret. Such types of bases need the special going near providing of their safety. Decision of question about determination of vulture of secrecy of documents, that distributing of information is after the categories of confidentiality, and also distributing of users on groups with the different levels of access and obmezheniyami in access to the electronic documents, that is determined the structure of organization and regular structure of podrozdiliv (chiefs, deputies, ordinary office workers, and others like that), testify to actuality of method which is offered authors.**

Ключові слова: **Безпека баз даних, відомості, що містять державну таємницю.**