18. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко. – К.: «МК-Прес», 2006. – 320 с.

19. Литвак Б.Г. Экспертные технологии в управлении: Учеб. Пособие. – 2-е изд., испр. и доп. – М.: Дело, 2004. – 400 с.

20. Дрейс Ю.О. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю / Ю.О. Дрейс, Н.С. Вишневська, Ю.Є. Хохлачова // Захист інформації. – Вип. №3 (48) – К.:НАУ. – 2010. – С. 87–94.

21. Дрейс Ю.О. Визначення рівня компетентності експертів експертної комісії з питань державної таємниці / Ю.О. Дрейс, О.Г. Корченко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: збірник наукових праць. – Житомир: ЖВІ НАУ, 2011. – Вип. 4. – С.190–196.

22. Інтелектуальна власність в науково-технічній діяльності: навчальний посібник / С.М. Злепко, І.С. Тимчик, С.В. Тимчик. – Вінниця: ВНТУ // [Електронний ресурс].– Режим доступу: http://posibnyky.vntu.edu.ua.

Надійшла: 03.07.2012 р.

Рецензент: д.т.н., професор Архипов О.Є.

УДК 004.738

Гумінський Р.В.

ВІРТУАЛЬНІ СПІЛЬНОТИ ЯК СУБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У статті проведено аналіз особливостей розвитку та характерних рис віртуальних спільнот, як суб'єктів інформаційної безпеки Держави. Розглянуто загрози інформаційної безпеки та інформаційний вплив віртуальних спільнот. Визначені напрямки протидії Держави від інформаційного впливу віртуальних спільнот та запропонована модель моніторингу віртуальних спільнот.

Ключові слова: віртуальні спільноти, соціальні мережі, інформаційна безпека, система моніторингу, інформаційні загрози.

Постановка проблеми. У сучасному інформаційному суспільстві відбувається зародження і становлення соціальних формацій – віртуальних спільнот (ВС), що володіють принципово іншими (в порівнянні з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями з надання впливу на традиційні громадські та державні структури, поява яких позв'язана з програмами створення оперативного доступу по каналах відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів в будь-якій точці земної кулі. Багато в чому поява таких ВС пов'язана з проведенням телекомунікаційної глобалізації.

Віртуальні спільноти (англ. virtual communities, e- communities) – новий тип спільнот, які виникають і функціонують в електронному просторі (перш за все за допомогою мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних задач, задоволення своїх інтересів у мистецтві, дозвіллі, тощо [1].

Термін «віртуальне співтовариство» (Virtual Community) запропонував Г.Рейнгольд, який надав йому таке визначення: «Віртуальні співтовариства є соціальними об'єднаннями, які виростають з Мережі, коли група людей підтримує відкрите обговорення достатньо довго і людяно, для того, щоб сформувати мережу особистих стосунків в кіберпросторі» [2]. Слід зазначити, що сам Г. Рейнгольд є одним із засновників одного з перших віртуальних співтовариств «The Whole Earth 'Lectronic Link» (WELL).

Сучасні ВС дослідники розділяють на декілька основних категорій [3]:

- співтовариства інтересів, які збирають людей з однаковими інтересами (такими, як політичні, соціальні, культурні, економічні тощо) або є спеціалізованими (співтовариства молодих батьків, клуби любителів певних марок автівок тощо);
- ігрові співтовариства, які дають своїм користувачам можливості створювати власне середовище, історії і персонажі в придуманих світах;
- географічні співтовариства, засновані на географічному розташуванні або місцевості (часто такі співтовариства об'єднуються за допомогою локальних мереж);
- співтовариства взаємин, які сформовані навколо певного життєвого досвіду, де люди можуть ділитися своїм досвідом і обмінюватися думками;

- комерційні співтовариства, де стосунки побудовані на купівлі та продажі онлайнових товарів і послуг;

- віртуальні держави.

Таким чином ВС в інформаційному просторі є принципово новою стійкою формою існування соціальних відносин, які перевершують соціальні соціуми за ступенем організованості та впливу.

За умов глобальної інтеграції головною ареною зіткнення національних інтересів держав стає інформаційний простір. А аналіз останніх конфліктів [4] засвідчили використання Інтернету для залучення до інформаційних операцій всесвітньої аудиторії. Зі зменшенням військових загроз та переходом в у невійськову площину, передусім в інформаційну сферу та розкладаючі загальні признаки суб'єктів інформаційного протистояння, а саме [5, 6]:

- наявність у суб'єкта в інформаційно-психологічному просторі власних інтересів;

- наявність у складі суб'єкта спеціальних сил (структур), функціонально призначених для ведення інформаційного протиборства або уповноважених на ведення інформаційного протиборства;

- володіння та/або розробка інформаційної зброї, засобів її доставки і маскування;

- під контролем суб'єкта знаходиться сегмент інформаційного простору, в межах якого він володіє переважним правом встановлювати норми регулювання інформаційно-психологічних відносин (на правах власності, закріплених нормами національного та міжнародного законодавства) або державним суверенітетом (національний сегмент інформаційного простору як частина державної території);

- існування в офіційній ідеології положень, що допускають участь суб'єкта в інформаційному протиборстві.

У зв'язку з цим поява в XXI столітті нової реальності у вигляді глобальних і соціальних мереж якісно змінюють середовище безпеки.

Аналіз останніх досліджень. ВС сучасні дослідники вивчають переважно або як соціальний феномен нової культури, що формується на засадах використання Інтернету, або з точки зору специфіки психологічних рис учасників таких спільнот, їх інформаційного наповнення, або з огляду на те, яку роль вони можуть відігравати у житті суспільства взагалі [7-12].

З погляду інформаційної безпеки держави дослідники визначають загальні риси суб'єктів інформаційної безпеки та надають загальні рекомендації щодо напрямків діяльності Держави, державних установ в інформаційному протиборстві [3,13].

Цілі статті. Метою дослідження є визначення характерних властивостей ВС, як суб'єктів інформаційної безпеки держави, правила протиборства Держави в інформаційному просторі соціальних мереж та побудови загальної моделі моніторингу та інформаційного протиборства Держави з ВС, як суб'єктами інформаційної безпеки.

Основна частина. Інформаційні загрози національної безпеки держави та властивості віртуальних спільнот, як суб'єкта інформаційної безпеки держави

Згідно до законодавства України поняття "інформаційна безпека" має таке визначення:

"*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.*" [14].

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України, які притаманні в Інтернет середовищі визначено в Доктрині інформаційної безпеки України [15]. При розгляді ВС, як суб'єктів інформаційної безпеки Держави доцільно розглядати наступні інформаційні загрози:

у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

- зовнішні негативні інформаційні впливи на суспільну свідомість;

у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;
- пропаганда сепаратизму за етнічною, мовною, релігійною та іншими ознаками.

Під інформацією в даному випадку необхідно розуміти в тому числі ідеї, мету існування а також ідеології, що служать чинником формування навколо них соціальних спільнот.

У відповідності до інформаційних загроз визначимо характерні риси ВС, як суб'єктів інформаційної безпеки держави:

1. за метою створення:

- створюються з метою досягнення визначених цілей на території вибраної держави або групи держав із елементів їх соціальних структур;

2. за структурою:

- включають в свою структуру, об'єднають матеріальні та інтелектуальні ресурси інших соціальних систем;
- мають ознаки децентралізованої ієрархії (принцип багатокерівництва), часткові лідери, кожний з яких має спеціалізовану роль і функцію;
- найбільші, глобальні за масштабами своєї діяльності та впливу на суспільні процеси мають ознаки суверенної держави - суверенітет; екстериторіальність; наявність власних силових структур; участь в міжнародних організаціях, що зближує їх стратегічні інтереси з національними інтересами традиційних держав, залучаючи до геополітичної конкуренції за сферами впливу;

3. за проникаючою та заповнюючою здатністю:

- миттєво отримувати з структур соціального суспільства і концентрувати розподілені інтелектуальні та матеріальні ресурси в будь-якій точці інформаційного простору;
- висока здатність заповнювати нестачу сил і засобів і втрати в інтелектуальних і матеріальних ресурсах, черпаючи їх прямо з соціальних структур (держав з розвиненою інформаційно-телекомунікаційною інфраструктурою), які не беруть участь в конфлікті на стороні даної віртуальної спільноти;
- мають проникаючу здатність в будь-які соціальні структури і, в разі залучення в інформаційний конфлікт (інформаційно-психологічну війну), здатні завдати своєму противнику удар зсередини, використовуючи його комунікаційні мережі та соціальні структури держави;

4. за здатністю реорганізації:

- при розпаді (наприклад, в результаті досягнення поставлених цілей або зміни пріоритетів) вона припиняє своє існування в якості самостійного суб'єкта міжнародної діяльності (або геополітичної конкуренції), а її структурні елементи повертаються на своє колишнє місце в ті соціальні системи, з яких вони були вилучені;
- здатні в найкоротші терміни повністю змінити свій вид, форму існування в інформаційно-психологічному просторі, свою структуру і методи діяльності, змінити внутрішню ієрархію і систему взаємодії та взаємовідносин окремих елементів усередині спільноти і в результаті цих змін взагалі стати іншим суб'єктом діяльності;
- володіють здатністю тимчасово припиняти своє існування, розчинятися в просторі соціальних систем;

5. за вразливістю:

- головною вразливістю віртуальних спільнот є ідеологія, що об'єднує розрізнені елементи в єдиний організм (систему) і створює мотивацію участі кожного з цих елементів у спільній діяльності з метою досягнення цілей під загальним централізованим віртуальним керуючим впливом.

Таким чином, ВС є ідеальним інструментом впливу на національні інтереси держави в інформаційному просторі.

Етапи розвитку віртуальних спільнот

На створення, діяльність та розвиток ВС впливають два фактору. Перший фактор - внутрішній, психологічний. Він визначає потребу людей з певним психологічним складом

доносити свої ідеї до оточуючих і намагатися схилити їх до своєї точки зору. Він же визначає об'єднання цих людей за ідеологічною ознакою у великі і малі групи. Другий чинник - зовнішній, селектуючий. Він визначає те, в який бік будуть спрямовані дії ідеологічних груп. Дія цього чинника полягає в тому, що правильні ідеологічні групи та їх дії, а також зручні лідери, заохочуються і розкручуються в інформаційному просторі, а невигідні, навпаки, залишаються без підтримки і заглушаються.

В своєму розвитку ВС проходить ряд типових етапів. Розглянемо етапи розвитку віртуальних спільнот як зростання популяції в залежності від часу існування (рис.1) [16].

Загальним для ВС буде начальна зона «сплеск популярності» приток популяції спільноти яка обумовлена людською цікавістю нових ідей. Деякий спад «лощина тих, хто сумнівається», зменшення популяції спільноти, відтік тих , хто не побачив подальшої зацікавленості в ідеології ВС. На цьому етапі проходить формування ядра ВС, розподіл функцій та ролей.

Далі проходить планомірний ріст популяції спільноти до її піку популяції ВС, зона стабільного існування і неминуче вимирання ВС або перехід в іншу форму існування.

Це загальні етапи розвитку ВС. Під час існування етапи розвитку можуть повторюватися декілька разів, або бути відсутніми в залежності від інформаційного наповнення та впливу.

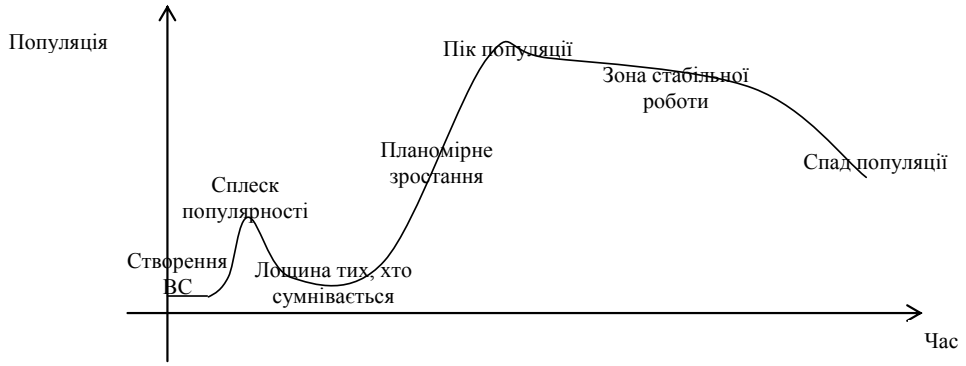

Рис. 1. Графік росту популяції ВС

Інформаційний вплив віртуальних спільнот на національні інтереси Держави

Соціально-мобілізаційна активність деструктивного характеру, а також акції протесту, що організовуються із застосуванням інструментарію соціальних мереж (рухи, демонстрації, флешмоби, перекриття трас тощо) стають повсякденними у житті сучасного суспільства.

Перевагами цього різновиду спільнот є небачена раніше оперативність, лабільність, доступність, ємність, а найголовніше – інтерактивність і мережна архітектура, що уможливлює і навіть стимулює необмежене зростання їхньої аудиторії.

Сценарій інформаційного впливу в Інтернет середовищі не відрізняється від класичних методів інформаційного впливу і починається з атаки на масову свідомість використовуючи класичні методи інформаційних війн:

- за цілями:
    1. Методи пропаганди.
    2. Методи контрпропаганди.

Методи пропаганди націлені на те, щоб донести до населення необхідні ідеї, тобто сформувати на певній ділянці інформаційного простору потрібні інформаційні сутності. Відповідно, методи контрпропаганди націлені на дискредитацію ворожих ідей, руйнування шкідливих інформаційних сутностей і недопущення їх виникнення в подальшому.

- за характером дії:
    1. Явні методи.
    2. Неявні (приховані) методи.

Явні методи відрізняються від неявних тим, що в них мета і характер впливу не ховаються від супротивника. Наприклад, агітація - це приклад явної пропаганди, а інформаційний вірус - прихованою.

ВС використовують засоби соціальних мереж, а саме:

- Форуми. Ця форма спілкування є розвитком ідеї телеконференцій. Повідомлення користувачів в форумах групуються по темах, які задаються, як правило, першим повідомленням. Історично перші форуми з'явилися як удосконалення гостьових книг і організовували повідомлення в гілці - так само, як і в телеконференціях. Як правило, теми групуються в тематичні форуми, управління системою здійснюють адміністратори і модератори. Найбільш розвинені форуми починають володіти першими ознаками соціальних мереж - між учасниками можуть бути встановлені соціальні зв'язки.

- Блоги (від англ. Web log - web-журнал, web-протокол). У цих сервісах кожен учасник веде власний журнал - тобто залишає записи в хронологічному порядку. Теми записів можуть бути будь-якими; найпоширеніший підхід - це ведення блога як власного щоденника. Інші відвідувачі можуть залишати коментарі на ці записи. У цьому випадку користувач, крім можливості вести свій журнал, дістає можливість організовувати стрічку перегляду - список записів з журналів друзів (friends), регулювати доступ до записів, шукати собі співрозмовників за інтересами. На базі таких систем створюються співтовариства - журнали, які ведуться колективно. У такому співтоваристві його членом може бути розміщене будь-яке повідомлення по напряму діяльності співтовариства.

Уже зараз потенціал ВС є достатнім, аби з їх допомогою влаштувати повномасштабний соціальний катаклізм, загальнонаціональну акцію, організувати громадський або політичний рух тощо. Згадуючи події 2012 року в Україні, що пов’язані із закриттям файлообменніку EX.UA можна стверджувати, що це був виклик національній безпеці.

Також необхідно зазначити на суттєвий вплив ВС на політику. Соціальні мережі полегшують можливість об’єднання осіб, що ставлять перед собою захоплення влади, у тому числі і незаконного.

Інтернет простір може використовуватися як місце спілкування, розробки і обговорення злочинних планів. Таке спілкування набагато безпечніше «фізичних» зустрічей в оффлайні. Крім того ВС можуть непомітно підривати деякі державні основи шляхом створення так званих «віртуальних держав», що мають майже усі атрибути держави за винятком території. Яскравим прикладом є революції в Тунісі, Лівії, Єгипті, Ємену, які призвели до усунення глав цих держав.

Але, коли ми кажемо про ВС як виклик національній безпеці не треба забувати, що існує «подвійна» роль віртуальних спільнот яка виявляється у тому, що вони водночас прискорюють та гальмують потенційне настання «революційної ситуації». Віртуальні спільноти можуть діяти як колективний симулятор протестного руху. Вони дуже часто створюють ілюзію опозиційної політичної активності, поглинаючи енергію, яка інакше могла б вилитися у «фізичні» протести на вулицях.

Правила протидії Держави від інформаційного впливу віртуальних спільнот

Досвід інформаційного впливу ВС переконливо свідчить про необхідність посиленої уваги з боку держави до діяльності та розвитку «соціальних мереж». Водночас, така увага не повинна порушувати права людини, зафіксовані у законодавстві.

Можна виділити такі напрямки щодо протидії інформаційного впливу ВС:

- силові методи – закриття серверів;
- юридично-правові методи – притягнення до кримінальної відповідальності учасників ВС;
- моніторинг ВС та протидія методами інформаційного впливу.

Перші два методи є більш ефективними в короткостроковій перспективі. Але їх недоліками щодо недопущення правопорушень в інформаційній сфері зумовлена багатьма об’єктивними причинами, які витікають з характерних властивостей ВС, як суб’єктів інформаційної безпеки, серед яких насамперед доцільно виділити:

1) відсутність географічних кордонів та обмежень для миттєвого поширення, збирання, обробки та використання інформації, внаслідок чого Інтернет з його глобальними комунікаціями залишається поза сферою правового регулювання законів будь-якої держави, яка завжди має певну обмежену територію, на яку поширюється її суверенітет (поняття юрисдикції або дії нормативно-правового акта у просторі);

2) анонімність, яка підриває традиційне застосування юридичної відповідальності за скоєне правопорушення або злочин в інформаційній сфері, що забезпечує високий рівень латентності та низький рівень розкриття правопорушень;

3) легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної документально оформленої інформації електронна інформація не має форми, сталої у часі та просторі.

Крім того, слід зазначити, що згідно чинного законодавства власники соціальних мереж не несуть значної кримінальної відповідальності щодо інформаційного наповнення.

Ще одно із проблемних питань щодо неефективності використання силових методів є те, що українські соціальні мережі дуже сильно інтегровані в російській або мировий Інтернет (з 10 найбільш відвідуваних сайтів в Україні – два українських).

Метод моніторингу віртуальних спільнот є більш ефективним в довгостроковій перспективі щодо інформаційної протидії ВС, але потребує залучення фахівців різних галузей науки. Використання цього методу дозволить не тільки знищення, придушення діяльності ВС але зміну ідеологій існуючих ВС

Модель моніторингу віртуальних спільнот

Система моніторингу ВС створюються з метою моніторингу Інтернет простору, аналізу розвитку та діяльності ВС та прийняття рішення щодо інформаційних ризиків та інформаційного впливу.

Виходячи із мети створення системи моніторингу ВС вона включає наступні підсистеми:

- підсистема моніторингу ВС;
- підсистема аналізу ВС;
- підсистема прийняття рішення;
- підсистема прогнозування;
- база знань.

На рис. 2. відображена структура системи моніторингу ВС та зв’язки між її підсистемами.

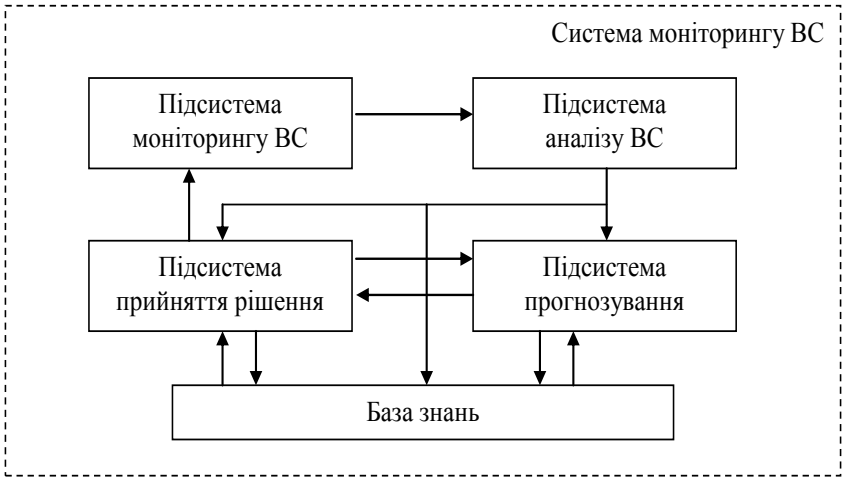

Рис. 2. Система моніторингу ВС

Підсистема моніторингу – призначена для моніторингу інформаційних ресурсів, згідно заданої тематики інформаційного потоку та надання статистичної інформації в підсистему аналізу ВС. Найбільш доцільно використовувати системи контент-моніторингу для оперативного аналізу інформаційної обстановки Інтернет середовища.

Підсистема аналізу ВС – призначена для аналізу ВС, її інформаційного наповнення, етапів розвитку та наповнення бази знань щодо розвитку ВС та її поведінки в залежності від інформаційного впливу.

Підсистема прийняття рішення – призначена щодо визначення інформаційних загроз; розробка пропозицій щодо інформаційного впливу; на підставі результатів прогнозування та

знань прийняття рішення щодо інформаційного впливу на ВС. В підсистему прийняття рішень можуть входити елементи систем прийняття рішень.

Підсистема прогнозування – призначена щодо прогнозування етапів розвитку ВС в залежності від інформаційного впливу за допомогою математичного апарату.

База знань – накопичення статистичних даних щодо розвитку ВС в залежності від інформаційного впливу та на підставі даної інформації формування правил розвитку та поведінки ВС.

Під час моніторингу ВС підсистемами аналізу ВС, прийняття рішення та прогнозування інформація про ВС спільноти передається в базу знань для створення статистики та формування правил. При цьому доцільно використовувати інформацію не тільки про ВС які представляють інформаційні загрози.

Висновки. Українське суспільство уже сьогодні достатньо глибоко інтегроване у міжнародні мережні віртуальні спільноти й вітчизняна аудиторія соціальних мереж збільшується рекордними темпами. Це зумовлює необхідність проаналізувати і оцінити динаміку, напрямки й тенденції даних процесів в Україні в контексті глобального розвитку соціальних мереж, дослідити глобальні громадсько-політичні рухи у соціальних мережах та їх вплив на політичні процеси сучасності.

Перед українською владою з розвитком соціальних мереж у контексті викликів національній безпеці постають наступні проблеми:

поява та структурізація віртуальних спільнот у вітчизняних соціальних мережах;

пошук та вироблення адекватних відгуків на кинутий виклик;

обмеженість механізмів державного регулювання даного соціального феномену, яка виявляється у спробах силової або адміністративної боротьби з новими викликами з боку органів державної влади.

Найбільш ефективним механізмів державного регулювання є моніторинг віртуальних спільнот (соціальних мереж) що ставить ряд наукових та організаційних задач перед державою, а саме: створення відповідних структур щодо моніторингу Інтернет середовища з залученням фахівців різних галузей наук, удосконалення та **розробка** науково-методичного апарату щодо аналізу, прогнозування розвитку та діяльності віртуальних спільнот.

ЛІТЕРАТУРА

1. Вікепедія: [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org.

2. Кремлева С. О. Сетевые сообщества / С. О. Кремлева. [Електронний ресурс] – Режим доступу: http://www.follow.ru/print.php?id=116&page=1.

3. Дзюндзюк В. Б. Віртуальні співтовариства: потенційна загроза для національної безпеки // Державне будівництво [Електронне видання]. – 2011. – № 1. – Режим доступу до журн. : http:// www.kbuapa.kharkov.ua.

4. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. М.: МОРФ, 2011,14 с.

5. Манойло А. В. Государственная информационная политика в особых условиях, монография. — М.: Изд. МИФИ, 2003, 388 с., ил.

6. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны, монография. — М.: Горячая линия — Телеком, 2003, 541 с., ил.

7. Белинская Е. П. К проблеме групповой динамики сетевого сообщества. 2-ая Российская конференция по экологической психологии. Тезисы. Москва, 12 – 14 апреля 2000 г. М.: Экопсицентр РОСС. - С. 249 – 251.

8. Войскунский А. Е. (1997) Групповая игровая деятельность в Интернете // Психологический журнал, т. 20. С. 126 – 132.

9. Иванов Д. В. Виртуализация общества // Социология и социальная антропология. СПб: Изд. „Петербургское Востоковедение”, 2000. 96 с.

10. Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология. Под ред. В. Л. Иноземцева, 1999. С. 494 – 505.

11. Круглов А. Ю. Компьютеро-опосредованное общение как социальное явление / Автореферат диссертации на соискание ученой степени кандидата социологических наук, Санкт-Петербург, 2000.

12. Нестерова Е. И., Нестеров В. Ю. Некоторые аспекты коммуникационных процессов в Сети с точки зрения культурологии // 5-я Международная научно-практическая конференция Информационные системы и технологии „Виртуальный мир Инфосферы: практическое использование человеком”. Владивосток, 1998.

13. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання, монографія. – К.: вид. Інтертехнологія, 2009, 163 с.

14. Конституція України.: прийнята на п'ятій сесії Верхов. Ради України 28 черв. 1996 р. – К. : Велес.

15. Доктрина інформаційної безпеки України : затверджена Указом Президента України № 514/2009 від 8 липня 2009 року [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/9570.html.

16. Сазонов В.М. Социальные сети – публичная сфера, монография. – М.: Изд. Лаборатория СВМ, 2011, 223 с., ил.

Надійшла: 11.07.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 629.735.05:621.3(045)

Мачалин И.А.

КРИТЕРИЙ ОПТИМИЗАЦИИ ПЕРИОДИЧНОСТИ КОНТРОЛЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Рассмотрена математическая модель процесса технического обслуживания телекоммуникационных систем. Предложен технико-экономический критерий оптимизации периодичности контроля работоспособности, учитывающий стоимостные характеристики и показатели достоверности контроля.

Ключевые слова: математическая модель, оптимизация, периодичность.

Постановка проблемы. В настоящее время широкое развитие телекоммуникационных систем (ТКС) приводит к внедрению новых сложных систем приема, передачи данных и коммутации. Качество предоставления телекоммуникационных услуг в значительной мере определяется техническим состоянием оборудования ТКС. Поэтому задача контроля технического состояния и своевременного устранения неисправностей ТКС является важной и актуальной.

Анализ исследований и публикаций. Решению этой проблемы посвящено ряд работ [1-3]. Ряд критериев оптимизации используют только надежностные и стоимостные показатели, однако не учитывают показатели достоверности контроля [1-2]. Те показатели, которые учитывают влияние достоверности средств контроля [3], используют в качестве основного показателя надежности среднее время наработки изделия на отказ. Для современных высоконадежных ТКС использование такого показателя не всегда оправдано, поскольку это приводит к завышенной оценке надежности. Авторами предлагается критерий, который учитывает показатель MTBUR (Mean Time Between Unscheduled Repairs) - среднее время наработки блока на досрочный демонтаж (восстановление) на интервале планирования обслуживания.

Цель работы и постановка задач. В соответствии с требованиями нормативных документов ТКС система должна контролироваться с определенной периодичностью. Целью настоящей работы является разработка критерия и алгоритма оптимизации периодичности контроля работоспособности (КР) систем.

В следствии конечной точности систем контроля, по результатам КР могут быть приняты ошибочные решения типа «ложный отказ» (работоспособная система ошибочно признается неработоспособной) или «необнаруженный отказ» (неработоспособная система ошибочно признается работоспособной). Известно, что при большой периодичности КР увеличивается вероятность события, при котором система может длительное время находиться в состоянии «необнаруженного отказа» (состояние в котором отказавшая система используется по назначению). Увеличение частоты КР позволяет существенно снизить среднее время нахождения системы в состоянии «необнаруженного отказа» за счет снижения уровня ошибок типа «необнаруженный отказ». Но это влечет за собой временные потери на КР и увеличение количества ошибок типа «ложный отказ», что в свою очередь приводит к увеличению вероятности досрочного демонтажа работоспособной системы. Таким образом, возникает необходимость определения оптимальной периодичности КР, позволяющей минимизировать потери вследствие ошибок КР. При этом ТКС конструктивно