Рисунок 4 – Спектральные характеристики различных методов сканирования
а – шумового поля Гаусса-Маркова
б – реальных изображений РО

Первый вывод, который можно сделать по результатам анализа состоит в том, что рекурсивные развертки Гильберта и Пиано гораздо лучше сохраняют корреляционные связи между элементами шумового изображения, чем различные традиционные развертки. Действительно, если в двумерном поле взять окрестность, содержащую τ элементов, то коэффициент корреляции между центральным и периферийными элементами составит $r^{\sqrt{\tau}}$. Подтверждением этого является экспоненциальное убывание автокорреляционных функций $R_p \approx r^{\sqrt{\tau}}$, а для традиционных разверток $R_t \approx r^{\tau}$. Энергетические спектры $F(n)$, полученные в результате преобразования Фурье экспериментальных автокорреляционных функций, свидетельствуют о том, что степень концентрации энергии на низких частотах выше для рекурсивных разверток, чем для любой из традиционных. Эта степень концентрации близка к той, которая получается при вычислении двумерного энергетического спектра исходного изображения. Корректность результата сравнения одномерного и двумерного спектров обеспечивается равенством n коэффициентов ряда для первого случая и ($\sqrt{n} \times \sqrt{n}$) для второго случая.

На рис. 3, б и рис. 4, б приведены аналогичные корреляционные и нормированные спектральные зависимости, полученные для реальных изображений РО. Среди приведенных результатов обращает внимание высокая степень корреляции для алгоритма радиально-круговой развертки, которая объясняется интегральным совпадением структуры изображения РО и структуры геометрического построения алгоритма сканирования.

IV Выводы

Рекурсивные алгоритмы сканирования с энергетической точки зрения наиболее предпочтительны для преобразования диффузных точечных изображений, которые не обладают свойствами регулярных структур либо свойства регулярности которых не определены в неявном виде. Другими словами, рекурсивные алгоритмы сканирования позволяют определить энергетические свойства изображений так же успешно, как и известные ортогональные преобразования.

Традиционные алгоритмы сканирования диффузных точечных изображений практически не различимы как по корреляционным, так и по спектральным характеристикам.

Отдельные методы традиционного сканирования структурированных изображений позволяют реализовать существенное сжатие видеоданных за счет выявления пространственной корреляции, используя методы группового или блочного кодирования.

Литература: ***1.*** *Форд Д., Понс Ж. Компьютерное зрение /– М., 2004.– 915 с.* ***2.*** *Рябова Л. В. Типовые операторы обработки изображений радужной оболочки глаза // Сб. научн. тр. НАУ «Защита информации», – К., 2006.– 15 – 18 с.* ***3.*** *Max T., Quantizing for minimum distortion // IRE Truns. Inf. Theory IT-16, 1980.– 7 – 12.* ***4.*** *Морелос – Сарагоса Р., Искусство помехоустойчивого кодирования / М., 2005. – 243 с.* ***5.*** *Ревенко В. Н. Комплексы средств отображения информации. – М., 1985.– 172 с.* ***6.*** *Катленд Н. Введение в теорию рекурсивных функций / М.:Мир, 1983.– 256 с.* ***7.*** *Климов Г. П., Кузьмин А. Д. Вероятность, процессы, статистика / М., 1985. – 232 с.*

УДК 354:007

БЕЗПЕКА КІБЕРПРОСТОРУ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ

Євген Скулиш, Дарія Прокоф'єва
Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

Анотація: **Розглянуті особливості проблеми забезпечення безпеки міжнародного кіберпростору, що створився завдяки розвитку сучасних інформаційних технологій в умовах глобального інформаційного суспільства.**
Summary: **The article represents the research of problems the defense of cyberspace in global society.**

Ключові слова: **Кіберпростір, інформація.**

І Вступ

Інформаційні технології охоплюють всі сфери суспільного розвитку, сприяючи вирішенню численних проблем – від створення нових форм спілкування громадян до переведення на якісно новий рівень обороноздатності держави. Водночас, розвиток та поширення інформаційних технологій полегшують доступ до них асоціальних та злочинних елементів. При цьому спостерігається наступна закономірність: чим складніше стає програмно-математичне забезпечення інформаційних систем та комп'ютерних мереж, тим вразливішими стають організаційні заходи та засоби захисту інформації в автоматизованих системах. Поряд із розвитком електроних засобів захисту інформації вдосконалюються і технічні засоби доступу до інформації, яка передається та обробляється в телекомунікаційних системах, її перехоплення, викривлення та знищення. Відповідно, зростає число протиправних діянь, які вчинюються у так званому кіберпросторі (віртуальному середовищі), що вочевидь є безпосереднім та неминучім наслідком глобалізації інформаційних процесів [1].

Власне глобальна інформаційна мережа Інтернет є основною складовою кіберпростору, який, однак, нею не вичерпується. В державних структурах, крупних корпораціях та у відносно малих групах користувачів, члени яких мають достатню кваліфікацію, створюються власні локальні мережі комунікацій. Однак за рахунок використання загальних алгоритмів інформаційних технологій, технічно можливим є доступ до вказаних мереж ззовні, а також їх об'єднання. Тобто, можлива міграція в указаних підпросторах, яка умовно дозволяє об'єднати їх під понятям кіберпростору. Необхідно також брати до уваги автоматизацію управління в різних сферах та зростання чисельності точок доступу до Інтернету – так званих «хот-спотів», поширення яких, за оцінками спеціалістів, в майбутньому викличе фактичну глобалізацію кіберпростору. Таким чином, слід констатувати, що розвиток інформаційних технологій, передусім Інтернет, призвів до того, що в умовах глобального інформаційного суспільства утворився ще один простір, який не є географічним в загальноприйнятому сенсі цього слова, однак повною мірою є міжнародним, так само, як це має місце щодо морського, повітряного та космічного просторів.

Сутність Інтернету як добровільного міжнародного об'єднання мереж робить найбільш природнім варіантом його регулювання механізм застосуваня договірних норм Інтернет-спільноти недержавними організаціями. Принциповим для ефективного розвитку глобального інформаційного суспільства є мінімально можливе державне регулювання суспільних відносин, пов'язаних з використанням та функціонуванням Інтернету. Розподіл сфер компетенції між вказаними недержавними організаціями та державами має будуватися за аналогією зі статусом саморегульованої автономії. Водночас, така політика регулювання Інтернета обґрунтовано має виключення у випадках, пов'язаних з міжнародною та національною безпекою, а також захистом прав та свобод людини і громадянина, якщо механізми саморегуляції виявляться недостатніми для врегулювання конфліктів [2].

При цьому Інтернет, як основна складова кіберпростору, продовжує асоціюватися з поняттям «середовища необмежених можливостей», які в аспекті свободи дій та висловлювань значно перевищують реальні можливості людини в соціальному просторі. Водночас, актуалізується і усвідомлення загроз, притаманних кіберпростору. Зокрема, це вплив некоректної або небезпечної інформації, неконтрольоване поширення порнографії, інформації, яка носить дискримінаційний характер або закликає до тих чи інших видів ворожнечі (расової, релігійної тощо), фінансові шахрайства з використанням он-лайн технологій, різнопланові терористичні атаки тощо. Так, наприклад, в поточному році представники парламенту Китаю звернули увагу на те, що секретна інформація про китайські військові технології досить часто з'являється на форумах, в блогах та чатах глобальної інформаційної мережі, що свідчить про необхідність посилити урядовий контроль за Інтернетом та цензуру в мережі. Відповідні заходи, спрямовані на боротьбу за «чистоту» кіберпростору, розпочаті Китаєм ще з 2004 року, забезпечили за цей час закриття десятків тисяч нелегальних інтернет-кафе, декількох тисяч сайтів непристойного змісту та сотень інших онлайнових ресурсів, які, на думку властей, можуть справити негативний вплив на політичну обстановку в країні [3].

Усвідомлення реальної та потенційної небезпеки вказаних загроз потягло за собою різнопланові зміни в структурі правоохоронних органів різних держав та в системі підготовки спеціальніх підрозділів, а також зумовили внесення істотних нововведень до національного законодавства та до організації зусиль міжнародної спільноти. Зокрема, під егідою ООН в 2005 році було створено Internet Governance Forum.

Враховуючи, що робота бізнесу, уряду та структур національної оборони переважно спирається на "інфраструктури інформаційних технологій", забезпечення безпеки якої набуває першочергового значення як наслідок значного зростання загроз у кіберпросторі, 2002 році було прийнято Закон про управління федеральною інформаційною безпекою (Federal Information Security Management Act of 2002, FISMA), який відображав намір США захистити власні комп'ютерні мережі [4]. Крім того, в 2002 році була розроблена

національна стратегія захисту кібернетичного простору, якою передбачалася необхідність забезпечення інформаційної безпеки на добровільній основі всіма користувачами Інтернет [5].

У національній стратегії США щодо захисту кіберпростору закладені три основні стратегічні мети:

- упередити кібератаки, спрямовані на критичні інфраструктури кіберпростору;
- знизити вразливість національного кіберпростору для кібератак;
- звести до мінімуму збитки від можливих кібератак та час, необхідний для ліквідації їх негативних наслідків;

У зв'язку з визначенням вказаних цілей виділено п'ять національних пріоритетів:

- система реагування на загрози національної безпеки кіберпростору, тобто створення такої системи заходів щодо швидкого виявлення загроз, сповіщення про атаки, обміну інформацією для координації заходів у відповідь та відновлення попереднього стану, яка має знизити шкоду від зловмисних дій у кіберпросторі; система повинна мати загальнонаціональний статус, в її створенні мають брати участь як урядові організації, так і приватні компанії;
- програма з попередження загроз національній безпеці кіберпростору та зниження його вразливості, тобто розширення та вдосконалення законодавчої бази, здатної забезпечити попередження кібератак та дій у відповідь, а також необхідність розробки заходів з оцінки вразливості кіберпростору (передусім – вразливості комп'ютерних програм) та забезпечення механізмів безпеки, що діють в Інтернеті;
- програма поглиблення знань про національну безпеку кіберпростору, оскільки вразливість кіберпростору багато в чому зумовлена недоліком знань про загрози кібербезпеці, що характерно для використання інформаційних систем на різних рівнях; з цією метою планувалося створення нових освітніх програм та розроблення умов видачі сертифікатів, які засвідчують отримання знань про основи кібербезпеки;
- охорона урядового кіберпростору, з урахуванням важливості якого пропонується підвищити рівень його захисту; заходи щодо захисту урядового кіберпростору мають стати зразком для застосуваня відповідних заходів в інших сферах, причому особливе значення надається стимулюванню розвитку ринкових відносин, що сприяють впровадженню в практику технологій з більш високим ступенем безпеки;
- національна безпека та міжнародне співробітництво з питань зміцнення безпеки кіберпростору; оскільки кіберпростір пов'язує США з рештою світу, що дозволяє зловмисникам завдавати удару на відстані в тисячі кілометрів, причому кібератаки фактично відбуваються з блискавичною швидкістю, що робить вкрай складним виявлення джерела загроз, вочевидь необхідність міжнародного співробітництва щодо зміцнення безпеки кіберпростору (зокрема, заплановано посилити роботу розвідувальних служб, вжити заходів щодо більш ефективного виявлення кібератак та відповіді на них, розширити координацію роботи з іншими державами з метою створення спеціальної мережі безперервного спостереження за кіберпростором, виявлення кібератак та їх можливого вчасного попередження) [1, 6].

Водночас, оприлюднений в 2003 році звіт про національну стратегію безпеки кіберпростору було піддано різкий критиці як такий, що носить переважно декларативний та рекомендаційний характер [7]. Також висловлювалися побажання щодо поглиблення наукового підґрунтя стратегії [8].

Керівництво держави звернуло увагу на те, що однією з центральних є проблема неефективності американської правоохоронної системи, зокрема, законодавства, оскільки останнє не відповідає масштабу загроз кіберзлочинності та кібертероризму, що сформувалися на сьогодні. Більше того, подальше просування в напрямку ринкової лібералізації сфери інформаційних технологій без адекватних засобів захисту національного кіберпростору і підвищення технічного рівня правоохоронної і судової системи є не лише нераціональним, але й небезпечним. Для протидії злочинності в сфері інформаційних технологій – захисту критичних елементів інфраструктури від кібертерористів, а користувачів – від різного роду он-лайнових шахрайств, забезпечення конфіденційності інформації, захисту прав інтелектуальної власності на елементи інформаційних технологій, копірайту тощо – необхідним виявився суттєвий розвиток всієї правоохоронної системи в цілому [9].

В березні 2007 року в сенатському комітеті США з питань збройних сил в рамках бюджетних читань було поширено доповідь, підготовлену міністром ВВС США М. Уінном та начальником штабу ВПС США М. Мослі. В доповіді повідомлялося про створення нового військового командуваня, яке отримало назву Кіберпросторове командування (Cyberspace command) і буде діяти спільно з Космічним та Повітряним командуваннями ВПС США. Основним завданням, що ставиться перед новою структурою, є забезпечення переваги США у кіберпросторі. Таким чином, США намагаються розвинути вже наявну в них перевагу у створенні новітніх технологій, фінансуванні сектора IT-розробок та контролю за Інтернетом для того, щоб досягти військового домінуваня в міжнародному кіберпросторі [10].

Про створення Кіберпросторогово командуваня стало відомо з листопада 2006 р. Командування буде розташовуватись на території бази ВПС США в Барксдейл, де за лінією військового застосування інформаційних технологій задіяні близько 25 тисяч осіб. Першим підрозділом, яке увійде до складу

командуваня, стане 67-е крило мережної боротьби, дислоковане на авіабазі Лекленд. В цілому нова структура буде створена на базі 8-ї повітряної армії ВПС США – стратегічного авіаоб'єднання. Очолить Кіберпросторове командування командир 8-ї армії генерал-лейтнант Р. Елдер. Фінансування нового командування має розпочатися з жовтня 2008 р., а остаточно оформити його структуру планується до 2009 р. Зокрема, передбачається, що воно може включати підрозділи розвідувальної служби ВПС. Крім того, Кіберпросторове командування буде виконувати свої завдання в координації з Космічним командуванням ВПС США та Командуванням війни в повітрі [11].

За визначенням Об'єднаного командування США, яке було поширене в 2006 р., під кіберпростором розуміється «місце, де електроний та електромагнітний спектр використовується для зберігання, модифікації та обміну даними через мережні системи та відповідні фізичні інфраструктури». За оцінками представників ВПС США, це формулювання дозволить новому командуванню працювати з такими загрозами, як відстеження фінансових потоків, використання GPS, радарів, засобів глушіння тощо. До завдань буде входити захист власних даних та пригнічення сторонніх джерел інформації.

Безпосередньо в указаній доповіді, яку було поширено в сенаті США, зазначається, що домінування в кіберпросторі виходить за рамки телекомунікацій та інформаційних технологій та вимагає домінування в усьому електромагнітному спектрі – від постійного струму до денного світла, включаючи радіхвилі, макрохвилі, інфрачервоне випромінювання, рентгенівські промені, спрямовану енергію, а також інші відповідні галузі. Також у вказаній доповіді зазначалося, що супротивники США вже використовують кіберпростір для проведення асиметричних атак. Це пов'язано передусім з невисокою вартістю входження в даний простір та використання його ресурсів. У зв'язку з цим однією із задач, яка стає перед Кіберпросторовим командуванням, є недопущення розовсюдження присутності супротивників США в цьому просторі [11 – 13].

В тому, що стосується кіберпростору, збройні сили США мають значно більшу перевагу, ніж лише значні фінансові асигнування. Історично склалося так, що саме на США припало найбільш бурхливе та підтримане державою зростання сектору інформаційних технологій, і, зрештою, саме США належить контроль за Інтернетом.

Починаючи з 1998 року за згодою Міністерства торгівлі США, імена доменів та інтернет адреси перебувають у розпорядженні компанії Internet Corporation for Assigned Names and Numbers (ICANN). Це дозволяє припустити, що нове Кіберпросторове командування буде мати досить широкі можливості у сфері роботи з Інтернетом. Тобто, фактично складається ситуація, коли окрема держава ставить під свій одноосібний контроль один з міжнародних просторів. Це викликає незадоволення цілої низки країн, зокрема, проти цього відкрито виступили Бразилія, Росія, Китай, ЮАР, Іран, Саудівська Аравія, Норвегія, Швейцарія тощо. Альтернативою одноосібного контролю над Інтеретом ці держави вважають створення при ООН органу, який би репрезентував інтереси всіх країн-членів цієї організації. Тобто, мова йде про те, що міжнародний простір має керуватися міждержавним органом, сформованим при міжнародній інституції, яка об'єднує більшість країн світу (подібна схема на даний момент вже сформована, наприклад, щодо іншого міжнародного простору – морського дна) [13 – 14].

Найбільш активно ідея міжнародного органу з питань контролю за Інтернетом при ООН почала обговорюватись на глобальному рівні після створення в 2005 р. на Всесвітньому інформаційному самміті (World Summit on Informational Society - WSIS) в Тунісі Internet Governance Forum, що діє під егідою ООН. Даний самміт збирається один раз на рік та обговорює найбільш актуальні питання в сфері інформаційних технологій та розвитку Інтернета. Слід зазначити, що в ході підготовки до першого форуму, який пройшов у 2005 р. в Тунісі, до вимог щодо створння міжнародного органу з питань управління Інтернетом приєднався ЄС. Як зазначили його представники, на даний момент США мають можливість одноосібного контролю за роботою глобальної інформаційної мережі, що переважно пов'язане з відсутністю відповідної міжнародної законодавчої бази. Натомість її створення та передача прав щодо управління Інтернетом міжнародному органу, який репрезентуватме інтереси всіх країн, що входять в ООН, є тим шляхом, який може забезпечити більш справедливе та безпечне використання даного простору. При цьому мову про безпеку слід вести не лише в контексті посилення контролю над можливостями використання інтернету та кіберпростору при вчиненні злочинів та терористичних атак, але й в контексті попередження будь-якого використання даного простору у військових цілях для забезпечення силового домінування однієї країни або групи країн над іншими. Зрештою, встановлення міждержавного контролю над міжнародними просторами від імені всіх країн-членів ООН та на базі цієї організації може стати однією з реальних можливостей для посилення позицій прибічників багатополярного світу та колективного підходу до мирного вирішеня міжнародних проблем і конфліктів. В цьому контексті створення міжнародного органу з питань контролю за Інтернетом або кіберпростором при ООН може стати плацдармом для перенесення досвіду на інші міжнародні простори [14].

Відповідно, в травні 2006 року Генсек ООН звернувся до світової спільности із закликом зміцнювати глобальну безпеку в кіберпросторі – починаючи зі сфери надання банківських послуг в режимі онлайн та закінчуючи сферою телемедицини, що дозволить повною мірою реалізувати потенціал інформаційно-комунікаційних технологій та прискорити процес розвтку, що зрештою знайшло відображення в створенні мережі ініціатив та вживати заснованих на інформаційно-комунікативних технологіях заходів у відповідь для підвищення безпеки та зміцнення довіри до використання вказаних технологій Консультативної групи, покликаної допомогти у скликанні Форуму з питань Інтернет-управління, метою якого є організація діалогу між зацікавленими учасниками з питань державного Інтернет-управління. Серед 46 членів Консультативної групи – представники урядів, приватного сектору та технічних спеціалістів з усіх регіонів світу [15].

Для нашої держави поки що не є характерним усвідомлення сутності кіберпростору як джерела та середовища продуціювання і розвитку загроз національній безпеці, а відповідно – не визначені й пріоритети міжнародного співробітництва з питань використання кіберпростору. На даний час Україна стала лише суб'єктом міжнародної співпраці у боротьбі зі злочинами у сфері комп'ютерних технологій (кіберзлочинами), ратифікувавши в 2005 році Конвенцію про кіберзлочинність від 23 листопада 2001 року [16]. Водночас, формування загальноєвропейського інформаційного простору вимагає від України передусім чіткої регламентації питань свободи слова, доступу до інформації, гарантій інформаційних прав людини, захисту персональних даних, контролю за транскордонною передачею інформації, свободи спілкування з використанням глобальної інформаційної мережі тощо [17], а також визначення безпеки кіберпростору та інформаційної сфери в цілому одним зі стратегічних пріоритетів національної безпеки не лише в соціокультурному, але і в політичному, військовому та правовому аспектах [18].

Література: ***1.*** *Ваганов П. А. Правовая защита киберпространства в //Правоведение. -2006. - № 4. - С. 73 – 88.* ***2.*** *С. Петровский (05.06.2005) Саморегулирование и госрегулирование в киберпространстве: выбор эффективных сфер компетенции [WWW документ]. URL: http://www.russianlaw.net/law/doc/a179.htm (15 вересня 2007).* ***3.*** *Китай опасается утечки военных секретов через Інтернет (12.03.2007) [WWW документ] URL: http://www. XAKEP.RU (15 вересня 2007).* ***4.*** *Principles and Challenges of the Federal Informalion Security Management Act (FISMA) (б/д)) [WWW документ] URL: http://wwwl.netsec.net/content/government/fisma/index.jsp (17 вересня 2007).* ***5.*** *Й. Эверс (2002) Киберпространство под федеральной защитой// Сети #20/2002 [WWW документ] URL:http://www.osp.ru/nets (27 вересня 2007).* ***6.*** *The National Strategy to Secure Cyberspace (2003) //[WWW документ] URL: http://www.whitehouse.gov/pcipb (17 вересня 2007).* ***7.*** *Б. Шнайер (2003). Американское киберпростанство: можем ли мы отразить нападение? Забудьте: пустой пиаровский документ содержит только рекомендации// [WWW документ] URL: :http://www.HackZona.Ru (27 вересня 2007).* ***8.*** *Berkovitz B., Hahn R. W. Cybersecurity: Who's Watching The Store? - p. 15-16.* ***9.*** *Е. Роговский, П. Шариков. О безопасности в киберпространстве http://www.pcweek.ru/Year2002/N40/ CP1251/Strategy/chapt3.htm (17 вересня 2007).* ***10.*** *США создает командование для ведения операций в "киберпространстве" (20.03.2007) [WWW документ] URL: http://www.rian.ru /world/america/20070320/62308635-print.html (17 вересня 2007).* ***11.*** *США формируют 1-й кибернетический фронт (07.11.2006) [WWW документ] URL:http://revolver.ru/internet/archive/2006/11/07 (17 вересня 2007).* ***12.*** *C. Todd Lopez. 8th Air Force to become new cyber command (2007) [WWW документ] URL:http://www.bestavia.com/eng/index.php?option=com_content&task=view&id=723&Itemid=37(17 вересня 2007).* ***13.*** *Международное киберпространство: милитаризация или демократизація (б/д) [WWW документ] URL:http://www.unitednations.ru/articles_25_1162284277.html (27 вересня 2007).* ***14.*** *Л. Сайфер. Китай обьявил Штатам кибер-войну (15.06.2007) WWW документ] URL:http:// www.utro.ru/articles /email/2007 /06/15/656067.shtml (17 вересня 2007).* ***15.*** *Вперед к глобальной безопасности киберпространства (20/05/2006) [WWW документ] URL:http://www.soyuz.by/second.aspx?document =18060&type =Qualifier&uid=6&page=41 (27 вересня 2007).* ***16.*** *Хахановський В. Г., Ращенко В. М. Проблеми реалізації в Україні положень Конвенції про кіберзлочинність у контексті міжнародної співпраці//Боротьба з організованою злочинністю і корупцією (теорія і практика). - № 14/2006 – С. 208-214.* ***17.*** *О. Соснін. Україні потрібна концепція національної безпеки//Урядовий кур'єр. - № 166 від 12.09.2007. – С.6.* ***18.*** *Президент України (12.02.2007) Указ Президента України «Про стратегію національної безпеки України» № 105/2007 від 12 лютого 2007 року [WWW документ]. URL http://www.rada.kiev.ua (20 вересня 2007).*

УДК 004.45