УДК 681.321;322:621.395

В.Г. Кононович

СОЦІАЛЬНИЙ ЗАХИСТ ІНФОРМАЦІЇ В КЛАСАХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Постановка проблеми. Системи захисту інформації в інформаційно-телекомунікаційних системах (ІТС), які раніше називали автоматизованими системами, стрімко розвиваються слідом за інформаційними технологіями. Посилюється вплив інформації на життя та діяльність людських спільнот у державі. Роль захисту інформації та інших інформаційних ресурсів в телекомунікаційних мережах, що використовуються в системах управління державою, суспільством, економікою, культурою значно зросла, але одночасно збільшились їх уразливість від різного роду загроз. Ефективність систем захисту суттєво залежить як від технічних факторів, так і, значною й вирішальною мірою, від людського (антропогенного) фактору. Це ставить проблему більш уважного вивчення ролі персоналу, користувачів, і взагалі людини у процесах захисту інформації, забезпеченні інформаційної безпеки діяльності особи, суспільства, держави, її економіки та виробництва на всіх рівнях. При цьому виникає необхідність уточнення загального підходу до захисту інформаційних ресурсів і до конкретних задач захисту.

Аналіз досягнень та публікацій. Основними принципами інформаційних відносин, визначеними Законом України "Про інформацію", є «гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації». Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість „вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій".

Законом України "Про захист інформації в автоматизованих системах" були визначені загальні вимоги щодо захисту інформації, політики в галузі захисту інформації, служби захисту інформації, тощо. За цим задачі захисту інформації в галузі зв'язку конкретизувались Законом України "Про зв'язок", що діяв до 2003 р. На цьому ж етапі була проведена стандартизація положень технічного захисту інформації державними стандартами ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97, ДБН *А.2.2-2-96* [1…4].

Значний науковий вклад в розвиток систем захисту інформації в ІТС України внесли своїми роботами Архипов А., Богуш В.М., Горицький В.М., Горбунко И., Домарев В.В., Заболотний В., Ємельянов С.Л., Конахович В., Мачусский Е., Новиков А.М., Поповский В.В., Персиков А.В., Савчук М. Хорев П., Хорошко В.О., Шорошев В., Юдін О.К.

Основи державної політики щодо безпеки України в інформаційній сфері визначені основоположним Законом "Про основи національної безпеки України" [5].

Закон передбачає такі основні напрями державної політики з питань національної безпеки в інформаційній сфері: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидій монополізації інформаційної сфери України.

Технічний захист інформації в ІТС детально нормується низкою нових вітчизняних нормативно-правових документів [6…9] та міжнародних рекомендацій [10, 11]. Системи захисту інформації багатьох країн – Китаю, Росії, США – розвиваються з урахуванням реалій інформаційних воєн [12]. В нормативних документах з технічного захисту інформації на

програмно-керованих АТС загального користування передбачається низка механізмів і заходів забезпечення гарантій захищеності інформації, які стосуються організаційних заходів роботи з персоналом [13…15]. Серед специфікацій гарантій захисту визначені рівні довіри до персоналу і, зокрема, передбачається дотримання вимог: до безпеки середовищ персоналу, до системи та контролю організації праці, до поведінки та контролю поведінки персоналу в робочий час та неробочий час. Методика оцінки захищеності інформації включає перевірку дотримання нормативних гарантій забезпечення захищеності інформаційних ресурсів експлуатаційного середовища, гарантій забезпечення інформаційної захищеності середовищ розробки та випробувань АТС, а також безпеки середовища творців АТС, середовища експлуатаційного персоналу.

В практику міжнародної стандартизації та в зарубіжних публікаціях введено поняття «соціальної безпеки» – societal security, обробки інцидентів з безпекою при забезпеченні безперервності функціонування та управлінні постійною готовністю [17].

Робота з персоналом в організаційній частині заходів захисту в чинній вітчизняній нормативно-правовій базі представлена у слабо систематизованому вигляді. Створився певний розрив між функціями систем захисту інформації з обмеженим доступом і задачами забезпечення національних інтересів в інформаційній сфері. Слід відмітити, що проблема захисту відкритої інформації поставлена зовсім недавно і часто ігнорується. Вважалось, що захистом секретної інформації та деякими обмеженнями можна забезпечити національну безпеку країни. Гігантські масиви відкритої інформації, важливої для суспільства і держави, залишаються не достатньо захищеними, а порядок, засоби й механізми захисту відкритої інформації залишаються не до кінця визначеними.

Ціль статті. Метою даної роботи є спроба ввести і обґрунтувати, в руслі системи забезпечення національної безпеки, необхідність класу системи соціального захисту інформації, визначити основні функції та задачі такої системи в умовах зростання ролі і впливу соціальної інформації на всі сфери життєдіяльності людини, суспільства та держави та, зокрема, на соціальний капітал.

Викладення основного матеріалу. Інформація відіграє провідну роль у всіх процесах функціонування інформаційного й постінформаційного суспільства. Існуючі системи захисту інформації орієнтовані, в основному, на захист інформації з обмеженим доступом. Відкрита інформація теж стає об'єктом захисту. Важливість її захисту та обсяги інформації, вимога щодо захисту якої встановлена законом, мають тенденцію до збільшення. В сучасних умовах з'явився феномен, так званої «соціальної інформації», роль якої важлива в контексті інформаційного протиборства та національної безпеки. Масове впровадження в усі сфери життєдіяльності людини, суспільства та держави новітніх інформаційних технологій, на жаль, супроводжується застосуванням нових технологій несанкціонованого доступу до інформації, її зняття та інформаційного впливу. При цьому розширюються зовнішні й внутрішні загрози інформаційної безпеки держави та її суб'єктів. Це зумовило глибинні зміни в системі інформаційної безпеки, як важливої складової національної безпеки держави, а також обумовило формування нових видів діяльності у сфері захисту інформації. Актуальність теми цієї роботи полягає в тому, що вирішення поставлених задач може підвищити ефективність систем захисту інформації в цілому. Ув'язавши воєдино всі аспекти захисту інформації можна знизити сумарні витрати на захист.

І Причини, за якими необхідно захищати відкриту інформацію

Є принаймні п'ять причини для захисту відкритої інформації: впровадження систем «електронного уряду», розвиток електронної торгівлі, застосування електронного документообігу й цифрового підпису, поширення операцій інформаційних війн та пояа феномену соціальної інформації.

Перша причина пояснюється появою посередника у відносинах між державними органами управління й органами самоврядування та населенням у вигляді мережі передачі даних чи Інтернет. Інформація може втрачати в мережах свої властивості цілісності,

доступності та спостережності внаслідок технічних недоліків обладнання, природних завад, помилок персоналу та навмисних атак зловмисників на мережу та інформацію. Це може приводити до серйозних негативних наслідків: втрати довіри до урядових установ, погіршенню керованості, порушенням громадського порядку тощо.

Одним з перших нормативно-правових документів, у якому поставлена вимога, що «об'єктом технічного захисту на програмно-керованих АТС (автоматичних телефонних станціях), а також на відомчих, корпоративних АТС є конфіденційна, а також відкрита важлива для особи, суспільства та держави інформація, яка зберігається та циркулює на цих АТС», став НД ТЗІ 1.1-001-99 [13]. На далі цю норму було закріплено в нормативно-правовому документі [8]. Визначено, що: «В автоматизованих системах повинен забезпечуватися захист від несанкціонованого доступу до державних інформаційних ресурсів з боку мереж передачі даних, зокрема глобальних мереж». «Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності комплексної системи захисту інформації (КСЗІ) вимогам із захисту інформації». Складовими державного інформаційного ресурсу, який має захищатись згідно діючого законодавства, є [7]: інформація, що становить державну або іншу передбачену законом таємницю; конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу; *відкрита інформація*, яка є власністю держави.

Друга причина витікає з потреб безпеки електронної торгівлі, яка використовується у комерційних відносинах не лише для торгівлі електронними товарами чи електронних платежів, а й торгівлі фізичними товарами. Вибір товару, замовлення й платежі виконуються електронними засобами, а доставка товару – фізичними засобами. Окрім захисту комерційної таємниці є необхідність захисту інформації, яка за своїм статусом відноситься до відкритої. В електронних комерційних відносинах небезпечними є порушення правильності ідентифікації та автентифікації об'єктів та суб'єктів цих відносин, втрата цілісності й доступності інформації та інших інформаційних ресурсів.

Третьою причиною є застосування електронного документообігу та цифрового підпису, які будуть охоплювати не лише конфіденційні, а й відкриті документи. Мова йдеться про надання електронному документу тієї ж юридичної сили, що й власноручно підписаному паперовому документу. Задачі підтримання цілісності, доступності електронного документа, невідмовності від авторства документа та невідмовності від його отримання, взаємної ідентифікації та автентифікації мають вирішуватись на всіх етапах створення, приймання-передавання, отримання, перетворення у форму, придатну для сприймання та зберігання.

Четверту причину можна віднести до найважливіших. Війна, як висловлювався німецький військовий та політичний діяч К. Клаузевіц, «є продовження політики іншими засобами». У 21 столітті робляться висновки, що «інформаційна війна є основним засобом сучасної світової політики, домінуючим способом досягнення політичної та економічної влади» [12]. Там же інформаційна війна визначається як «спосіб організації ноосфери й світового інформаційно-психологічного простору у своїх інтересах». Масова комп'ютеризація, впровадження й розвиток інформаційних технологій привели до зростання інформаційного протиборства у політичній сфері. Управління інформаційними потоками перетворилось у вирішальний фактор завоювання, зберігання та утримання влади. Інформація є основним інструментом влади. Інформаційна війна, як і війна гаряча, має в своєму арсеналі й аморальні методи: обман, брехню, напівправду, підтасовку, замовчування та перекручування фактів тощо. Метою інформаційного протиборства є порушення інформаційної безпеки ворожої держави, цілісності чи стійкості системи її державного й військового управління, ефективний інформаційний вплив на керівництво, політичну еліту (тобто індивіди, які володіють найбільшим багатством, впливом, найвищим статусом), системи формування суспільної думки та прийняття рішень, а також забезпечення власної інформаційної безпеки для завоювання інформаційної переваги у інформаційному просторі.

У інформаційному протиборстві в сфері світової політики захист відкритої і закритої інформації стає одним з вирішальних факторів. За висновком провідного китайського теоретика інформаційної війни Шень Вей Гуана: «Щоб захистити політичну безпеку країни, треба навчитись вести інформаційну війну з використанням різних засобів масової інформації (ЗМІ). Крім того, необхідні заходи, засоби й технології захисту від несанкціонованого несприятливого інформаційно-психологічного впливу [12].

Розрізняють два види інформаційної боротьби: інформаційно-технічну та інформаційно-психологічну. При інформаційно-технічній боротьбі головними об'єктами впливу і захисту є інформаційно-технічні системи: системи зв'язку, телекомунікації, радіоелектронні засоби тощо. При інформаційно-психологічній боротьбі головними об'єктами впливу й захисту є психіка політичної еліти, персонал стратегічно важливих об'єктів та населення, системи формування суспільної свідомості, думки та прийняття рішень, соціальні об'єкти: окремі індивіди, соціальні групи, суспільство, держава, світове співтовариство. Інформаційна боротьба має вестись на трьох рівнях: стратегічному, оперативному, тактичному. На стратегічному рівні мають діяти, в основному, органи державної влади, на оперативному рівні – спецслужби та великий капітал, на тактичному та оперативному рівнях – керівництво суспільних та виробничих формувань.

П'ята причина захисту відкритої інформації тісно зв'язана з попередньою причиною. Девізом інформаційного суспільства є інтелектуальна конкурентно спроможність. У інформаційному суспільстві більше половини робочого часу буде використовуватись на зберігання, обробку й передачу інформації. Спостерігаються неймовірні прискорення приросту знань людства. У 70 роки 20 століття обсяг знань людства збільшувався вдвоє за 10 років, у 80-і роки – раз у 5 років, до кінця 90-х років обсяг знань людства подвоювався практично кожен рік [12, с. 7]. Прискорення інформаційних процесів, посилення комунікативності й ціле направленості взаємодій підвищує живучість індивіда, спільнот, суспільства, соціальних систем, але й створює нові вразливості. В сучасних умовах з'явився феномен, так званої «соціальної інформації», роль якої важлива в контексті інформаційного протиборства та національної безпеки і яка потребує захисту.

II Соціологічна, соціальна інформація та соціальний капітал

Під інформацією Закон України «Про інформацію» розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі. Обмін інформацією може здійснюватись технічними та програмними засобами телекомунікаційної системи шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Основними видами інформації, у визначенні Закону України "Про інформацію", є статистична, правова, соціологічна інформація, інформація довідково-енциклопедичного характеру, яка використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами, а також масова інформація та інформація про особу.

Соціологічна інформація – це документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів. Джерелами цієї інформації є відомості, в яких відображено результати соціологічних опитувань, спостережень та інших соціологічних досліджень.

На відміну від соціологічної інформації, *соціальна інформація* безпосередньо функціонує у людському суспільстві, відіграючи в ньому управляючу роль в процесах життєдіяльності й взаємодії з оточуючим середовищем. Феномен соціальної інформації відображається як атрибутивна та функціональна складові. Атрибутивна складова соціальної інформації служить для задавання понять, визначень, правил, думок, цінностей, символів, міфів та

інших атрибутів дійсності та життєдіяльності. Комунікативна складова соціальної інформації є засобом встановлення, організації та здійснення взаємодії суб'єктів інформаційних відносин в процесі їх діяльності в умовах суспільних відносин та оточуючого середовища. Функціональна складова соціальної інформації необхідна для повсякденної діяльності, праці, аналізу, прийняття рішень та задоволення нагальних фізичних, емоційних, інтелектуальних та психологічних потреб.

Суспільство і держава має посилити увагу до інформаційного забезпечення.

Класифікацію соціальної інформації надано в [12, с. 8]. Соціальну інформацію поділяють на три типи: про сучасність, про минуле, про майбутнє. Соціальна інформація може бути прогностичною (з функціями: орієнтовної, нормативної, попереджувальної) та плановою. За видами соціальна інформація може бути внутрішня та зовнішня, горизонтальна та вертикальна (пряма – директивно-нормативна, зворотна – контрольно-звітна, зокрема соціологічна).

Функціонування соціальної інформації характеризують наступними ознаками:

- за рівнями циркуляції: національний, регіональний, континентальний, глобальний;
- за часом циркуляції: короткострокове, середньострокове, довгострокове;
- за коментарями до інформації: позитивними, негативними, нейтральними;
- за способом доведення інформації: за допомогою ЗМІ, через спецслужби, через неформальні зв'язки, за допомогою дипломатичних джерел, через бізнес-структури;
- за метою доведення інформації: переконання, вплив, реакція у відповідь, компрометація, створення нових цінностей та правил для спільнот чи еліти.

Важливу роль у людських спільнотах відіграє соціальний капітал, у формуванні якого одну з провідних ролей несе соціальна інформація. Поняття соціального капіталу в інформаційному суспільстві було додатково введено як економічна й, одночасно, соціологічна категорія до раніш існуючих фізичного та людського капіталу. Як відомо, фізичний капітал складають земля, будівлі, машини. Людський капітал виражається у вміннях, знаннях у головах людей. Соціальний капітал, подібно до фізичного і людського капіталу створює багатства, а тому має економічну цінність для національної економіки. Властивості соціального капіталу та його роль вивчаються у економічних, соціальних, політичних та культурних процесах [19…21].

Соціальним капіталом називається сума спільних суспільних вартостей, таких, що дійсно стали спільними – це набір неофіційних вартостей чи норм, які є спільними для членів групи і дозволяють їм взаємодіяти. Соціальний капітал відіграє суттєву роль у забезпеченні ефективності функціонування суспільства. Соціальний капітал формується добровільно, основується на неписаних законах, формується шляхом самоорганізації соціальних груп, для його підтримання не потрібно застосування сили чи примушування з боку держави, його проявами є соціальне партнерство. Соціальний капітал утворює сферу образу життя, відображає спосіб взаємодії соціальних груп і її членів в середині групи.

З прискоренням технологічного та інформаційного прогресу змінюється рівень маніпулювання людьми, людина стає менш захищеною, розвиваються методи соціальної психології та інформаційного впливу на людей. Необхідно управляти соціальним капіталом та враховувати соціально-політичні наслідки впливу на соціальний капітал. В системі діагностики соціального капіталу та соціальної інформації збирають дані стабільності соціальних показників суспільства: здоров'я, громадської безпеки, освіти, праці (вибір цінностей, вдоволеність працею), доходів, житла, дозвілля та відпочинку, демографії.

III Загрози соціальній інформації та соціальному капіталу

Закон України «Про основи національної безпеки» [5] визначає основні засади гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз національним інтересам і національній безпеці України в усіх сферах життєдіяльності. В інформаційній сфері виокремлено загрози: прояви обмеження свободи слова та доступу

громадян до інформації; комп'ютерної злочинності та комп'ютерного тероризму; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Кожен з багатьох видів відкритої інформації має свою специфіку загроз. Тут зосередимось на загрозах соціальній інформації та соціальному капіталу.

Національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам [5]. Національні інтереси – це життєво важливі матеріальні, інтелектуальні і духовні цінності українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток. Коротко формулюється завдання захисту національних інтересів у США – це захист народу, території та образу життя.

Національна безпека України залежить від цілісності, доступності й спостережності відкритої інформації. надійності й готовності критичних фізичних та інформаційних інфраструктур. Соціальна та інша відкрита інформація важливі для держави настільки, що їх спотворення або знищення можуть привести до згубних наслідків в області економіки, оборони, охорони здоров'я та національної безпеки. Стає великою залежність всіх технологій від загроз інформаційним технологіям і вразливості останніх. Програмно-математичний вплив на інформаційно-комунікаційні системи, так звані комп'ютерні атаки, засоби інформаційного протиборства направлені на використання, модифікацію, підміну або знищення інформації, яка міститься у комп'ютерах та інформаційних мережах, зниження ефективності функціонування або виведення з ладу самих комп'ютерів та інформаційних мереж. До них відносяться засоби несанкціонованого доступу, комп'ютерні віруси, програмні закладки, «логічні бомби» та «троянські коні», нейтралізатори тестових програм, навмисне створені приховані інтерфейси для входу в інформаційну систему з корисними або диверсійно-підривними намірами, створення непомітних завад інтелектуального впливу на системи зв'язку, збирання та обробка інформації шляхом блокування, підміни у повідомленнях ключових елементів, введення у повідомлення хибних ключових елементів.

Завади інтелектуального впливу треба враховувати у системах забезпечення безпеки суспільно політичних відносин в рамках забезпечення національної безпеки. Вони базуються на автоматизованому аналізі структури повідомлень, слідкуванні за ключовими словами, синтезі мови у реальному масштабі часу. Небезпека таких загроз у тому, що фальсифікація може проводитись не лише власником чи розпорядником інформації, за що він має нести відповідальність перед законом, а й противником, приховано, під час передачі інформації телекомунікаційною мережею. Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації приводять до широкомасштабних наслідків у політичному, релігійному або ідеологічному планах. Інформація викрадається, перекручується, обмежується, фільтрується з метою впливу (або несанкціонованого виключення впливу) на психіку людини, психологію великих мас людей, суспільну свідомість з метою примусити їх думати і діяти в напрямі, потрібному для того, хто організує та здійснює цей вплив [18].

Можна припустити, що рівень небезпечності загроз цільового інформаційного впливу прямо пропорційний рівню технологічного розвитку мереж та масштабам застосування комп'ютерів у системах управління мережею, галуззю і державою в цілому. Зростає важливість вимог забезпечення цілісності та достовірності передачі відкритої інформації, захисту від порушень правил маршрутизації, точності й своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого

доступу до інформаційних ресурсів мереж та забезпечення фізичної безпеки інформаційної інфраструктури. Безпека інфраструктури держави в цілому залежить від рівня безпеки державних і комерційних інформаційних та телекомунікаційних систем.

З початком інформаційної ери з'явився й інформаційний тероризм, який має два різновиди: інформаційно-психологічний та інформаційно-технічний. Інформаційно-психологічний тероризм орієнтований на використання різних форм та методів впливу на інформаційно-психологічне середовище. Він характерний цілеспрямованим використанням ЗМІ для створення у суспільстві особливого психологічного становища, яке несе катастрофічні наслідки для життєдіяльності інформаційно-психологічного середовища суспільства й держави.

Інформаційно-технічний тероризм – це нанесення збитків окремим фізичним елементам інформаційного середовища держави: наведення завад, використання руйнівних програм проти систем управління, або зовнішнє несанкціоноване управління технічними об'єктами, хімічні та біологічні засоби руйнування, знищення ліній зв'язку, неправильна маршрутизація, штучне пере завантаження вузлів комутації тощо.

Інформаційні ресурси мають бути надійно захищені від негативних інформаційних впливів: мають бути виключені можливості для підміни або знищення соціальної інформації з найважливіших питань образу життя народу України.

IV Поняття про систему соціального захисту інформації

Законодавством визначені поняття криптографічного та технічного захисту інформації.

Криптографічний захист інформації (КЗІ) – це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховання/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [5]. Клас систем КЗІ можна представити *рис. 1а*, на якому наглядно показано характерне співвідношення нерозривних складових класу: криптографічних засобів, технічних засобів та організаційних заходів захисту. Криптографічний захист інформації застосовується для захисту інформації, яка передається каналами зв'язку або зберігається в базах даних, робочих станціях, міститься у парольних та ключових даних систем аутентифікації та розмежування доступу. Споживачами послуг системи КЗІ є суб'єкти органів державного управління, оборони, надзвичайних ситуацій, правопорядку, національної безпеки, розвідки тощо.

Технічний захист інформації (ТЗІ) – це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [6]. Він реалізується системою ТЗІ, яка згідно державного стандарту [3] є сукупністю організаційних структур, нормативно-правових документів та матеріально-технічної бази, що, в свою чергу, складається з таких елементів: захищені технічні засоби, засоби ТЗІ та засоби контролю за ефективністю ТЗІ. Таким чином, клас систем ТЗІ можна представити *рис. 1б* з характерним співвідношенням його складових: технічних засобів, організаційних заходів захисту та криптографічних засобів (за необхідності). Криптографічні заходи мають тут обмежене, але невід'ємне застосування – для захисту інформації, що зберігається на носіях та передається каналами зв'язку між елементами інформаційної системи. Серед організаційних засобів захисту необхідну і суттєву роль відіграють послуги та механізми захисту, які пов'язані з персоналом.

Клас систем ТЗІ застосовується в інформаційно-технічній боротьбі з метою захисту інформаційного середовища суспільства та захисту об'єктів інформаційної діяльності (ОІД) за принципом «кругової оборони». Споживачами послуг системи ТЗІ є, в основному, підрозділи, які захищають інформацію з обмеженим доступом, комерційні структури, банки.

З міркувань симетричності, яка є одною із фундаментальних властивостей природи, та почуття естетичності функціональної повноти класів систем захисту інформації, яке по праву вважається критерієм правильності технічних рішень, а також потреб практичної діяльності має бути реалізований клас систем захисту інформації, в якому головну роль, поряд з технічним та криптографічним забезпеченням системи захисту, відігравали б соціально-психологічні організаційні засоби – робота з персоналом, користувачами, кадровим забезпеченням, тобто в якому головна увага приділялась би людському фактору. Характерне співвідношення складових такого класу систем захисту наведене на *рис. 1в*.

Криптографічні засоби забезпечують захист відкритої інформації в системах електронного документообігу, цифрового підпису та технологічної і приватної інформації.

У відповідності з методологічним принципом – бритвою Оккама – не слід створювати суттєвості без необхідності. Але в даному разі є вагомі обґрунтування введення поняття ще одного виду захисту – соціального захисту інформації (СЗІ). З численних статистичних даних випливає що до 60% інцидентів з інформаційною безпекою пов'язані з людським фактором: помилки чи некомпетентність персоналу та користувачів, зловмисні та незловмисні дії, підкуп персоналу, порушення корпоративної солідарності тощо.

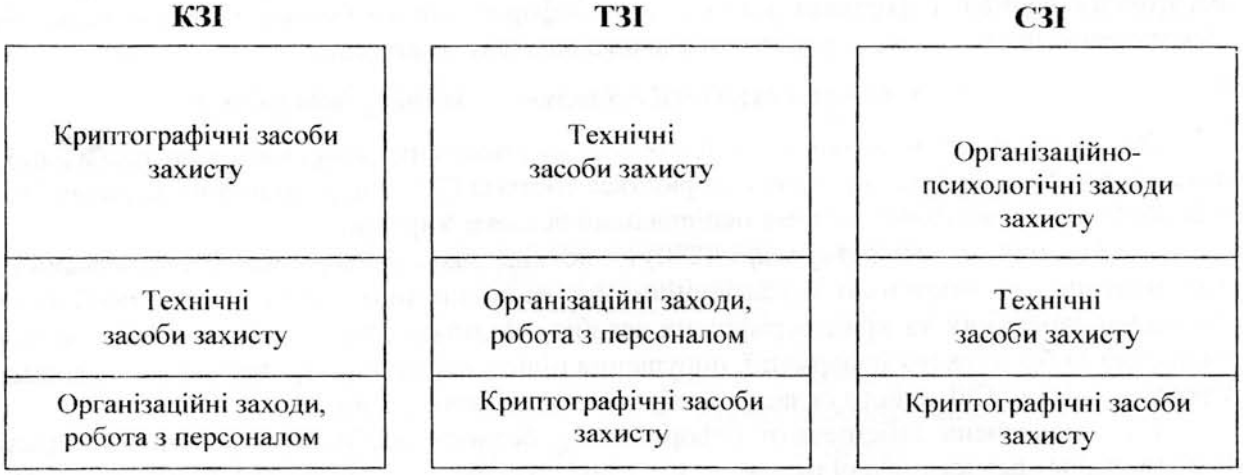

Рис. 1. Класи та складові класів систем захисту інформації

Є особливості в методах захисту відкритої інформації у порівнянні із захистом інформації з обмеженим доступом. До цих особливостей можна віднести:

1) значний обсяг відкритої та закритої інформації, які підлягають захисту, що вимагає застосування автоматизованих систем і засобів захисту;

2) переважання короткоживучої інформації, що приводить до зменшення строків її обробки та запам'ятовування в системі;

3) зростання ролі соціальної інформації в підтримці і забезпеченні національної безпеки, що посилює необхідність її захисту.

СЗІ забезпечують проведення організаційно-психологічних заходів для захисту соціальної інформації. Системи СЗІ мають функціонувати на об'єктах інформаційної діяльності органів державного управління та самоврядування, фірмах та підприємствах будь-якої форми власності, суспільних організаціях, об'єднаннях громадян тощо. Споживачами послуг системи СЗІ є суб'єкти системи національної безпеки, органів державного управління, систем інформаційної безпеки комунікацій (транспорту, енергетичних мереж, паливо-проводів, зв'язку), систем забезпечення життєдіяльності, оборони, надзвичайних ситуацій, правопорядку, промислових об'єктів тощо.

Системи КЗІ, ТЗІ, СЗІ взаємо зв'язані одна з одною. Вони можуть бути складовою частиною інших систем безпеки: економічної безпеки, екологічної безпеки, енергетичної, продовольчої безпеки тощо. Найбільш важливою є взаємодія головних систем безпеки

держави: національної безпеки, безпеки інформаційного простору, криптографічного, технічного і соціального захисту інформації (*рис. 2*).

Рис. 2. Головні системи безпеки держави

Політика безпеки соціальної інформації має передбачати наступні задачі захисту: підтримка властивостей цілісності і доступності соціальної інформації; попередження негативних впливів інформації з точки зору інформаційного протиборства; інформаційне забезпечення процесів відтворення соціального капіталу в державі.

V Основи стратегії соціального захисту інформації

Для захисту від негативних наслідків впливу соціальних об'єктів в ході глобальної чи локальної інформаційної боротьби створюється система СЗІ та інформаційно-психологічного забезпечення як складової частини національної безпеки України.

Соціальний захист інформації (СЗІ) – це вид захисту інформації, спрямований на забезпечення за допомогою організаційних та психологічних заходів, а за необхідності інженерно-технічних та криптографічних засобів, унеможливлення впливу на інформацію, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Спосіб реалізації СЗІ та його склад потребують подальшого уточнення.

СЗІ призначена забезпечити інформаційну безпеку особи, суспільства та держави. Інформаційна безпека суспільства – це стан захищеності інформаційного середовища суспільства, яке забезпечує його формування й усталений розвиток в інтересах громадян та держави. При цьому, під інформаційним середовищем розуміють сукупність інформаційної інфраструктури, інформаційних ресурсів, систему формування, зберігання, розповсюдження, використання і захисту інформації.

Загроза інформаційні безпеці – це фактори чи їх сукупність, які створюють небезпеку функціонуванню та розвитку інформаційного середовища суспільства, організації, підприємства. Подібно тому, як ТЗІ є необхідним при забезпеченні правил обробки документів, які містять державну таємницю, так і СЗІ є необхідною при забезпеченні правил обігу й обробки соціальної й іншої відкритої інформації, та організації роботи з персоналом.

СЗІ захищає соціальну інформацію при забезпеченні психологічної безпеки еліти, персоналу та населення України. Система СЗІ не є ні ідеологічною системою, ні політичним органом. Хоча одним із її побічних призначень є необхідність, хоча би частково, замістити вакуум, який утворився після краху соціалістичної ідеології та радянської політичної системи, у питаннях організаційно-психологічної роботи з персоналом, захисту соціальної інформації і підтримки соціального капіталу суспільства та забезпечення відтворення соціального капіталу в рамках інформаційної безпеки країни та її суб'єктів.

Система СЗІ не підміняє собою керування персоналом чи соціальний захист суб'єктів. Соціальний захист – система заходів й відповідних інститутів, призначених для захисту різних прошарків населення від економічної і соціальної деградації, пов'язаної з безробіттям, втратою або різким скороченням доходу, виробничою травмою, або професійним

захворюванням, хворобою, інвалідністю, старістю, втратою годувальника, народженням дитини і т. п. Система СЗІ забезпечує захист соціальної і зокрема соціологічної інформації.

Система СЗІ не відіграє другорядну роль у веденні інформаційного протиборства. Інформаційне протиборство – це форма боротьби сторін, при якій використовуються спеціальні – політичні, економічні, дипломатичні, військові тощо – методи, способи й засоби для впливу на інформаційне середовище противної сторони та захисту власної в інтересах досягнення поставлених цілей.

Інформаційно-психологічний вплив є ціле направлене виробництво та розповсюдження спеціальної інформації, яка спричиняє безпосередній позитивний чи негативний вплив на соціальний капітал, на функціонування та розвиток інформаційно-психологічного середовища суспільства, психіку та поведінку політичної еліти, персонал економічної й технічної інфраструктури та населення країни.

Завданням і цілями СЗІ є захист інформаційних ресурсів в інформаційній сфері від несанкціонованого доступу, зокрема соціальної інформації, та забезпечення безпеки інформаційно-телекомунікаційних та електронних системах, де вона циркулює.

Місце СЗІ серед систем протидії загрозам безпеки держави показано на *рис. 3.* Відносно захисту від інформаційних впливів та захисту інформаційного простору системи КЗІ, ТЗІ, СЗІ займають рівноправне положення. При цьому система СЗІ має завдання захисту, головним чином, соціальної інформації та соціального капіталу.

Сфера СЗІ нормується державою, підконтрольне державі та суспільству і створюється для забезпечення національної безпеки, усталеного розвитку суспільства і людини в умовах інформаційних воєн та інформаційного впливу.

Рис. 3. Місце СЗІ в системі протидії загрозам безпеки держави

Задачами СЗІ на державному рівні є:

- захист від засобів небезпечного впливу на інформаційну сферу;
- протидія маніпуляціям суспільної свідомості та формування очікувань суспільної свідомості;
- протидія (виявлення та обробка інцидентів) з порушенням нормального функціонування інформаційно-телекомунікаційних систем;
- забезпечення цілості інформаційних ресурсів, включаючи цілість захищаємої інформації, цілісності засобів обробки, зберігання та передачі інформації, прийнятного рівня соціального капіталу та персональних соціальних показників персоналу;
- протидії отриманню несанкціонованого доступу до інформаційних ресурсів;
- протидія порушенням прав та свобод громадян та юридичних осіб;
- сприяння створенню соціально-економічних умов для здійснення творчої діяльності;
- вироблення форм та засобів суспільного контролю за формуванням у спільнотах духовних цінностей, які відповідають національним інтересам країни, вихованням громадянської та корпоративної відповідальності;

- розробка дійових організаційно-правових механізмів доступу ЗМІ, співробітників та громадян до відкритої інформації про діяльність органів державного управління та місцевого самоврядування, підприємств, організацій;
- розробка спеціальних правових , організаційних і технічних механізмів недопущення протиправних інформаційно-психологічних впливів на масову свідомість суспільства, спільнот і колективів, раціонального використання накопичених суспільством інформаційних ресурсів;
- протидія пропаганді насилля й жорстокості, анти суспільній поведінці, впливу іноземних релігійних організацій;
- діагностика та захист соціальної інформації;
- аналіз та збирання даних оцінки соціальної інформації, соціального капіталу та процесів які проходять у зовнішньому середовищі.

В класі систем ТЗІ розглядаються канали витоку інформації та канали впливу на інформаційні ресурси. Каналами витоку інформації є технічні, антропогенні канали витоку та канали несанкціонованого доступу. Вплив на інформацію та інші інформаційні ресурси здійснюється технічними каналами. Захисту підлягають інформаційні ресурси і, зокрема, інформація.

В класі СЗІ, крім технічних каналів впливу на інформаційні ресурси, розглядаються інформаційно-психологічні канали впливу на суб'єкти інформаційних відносин. Захисту підлягають інформаційний простір держави, інформаційне середовище суспільства та людини, а також інформаційні ресурси. Мірою ефективності СЗІ можуть бути показники якості соціального капіталу та його відтворювання, результати аналізу соціальної інформації.

Місце СЗІ серед систем забезпечення безпеки показано на рис. 4.

Рис. 4. Місце системи СЗІ в системах забезпечення безпеки

Зауважимо, що системи КЗІ та ТЗІ є складовими систем забезпечення: національної безпеки; безпеки технологічних комунікацій; безпеки економічної фінансової, екологічної тощо; безпеки інформаційно-телекомунікаційних систем. Система СЗІ, крім того, є складовою частиною безпеки національного інформаційного простору, соціального захисту суспільства та суспільних об'єднань (соціального капіталу) та соціального захисту особи

СЗІ створюється на всіх рівнях: держави, суспільних організаціях та спільнотах, підприємствах, організаціях, фірмах. До фахівця системи СЗІ мають бути такі вимоги: здійснювати постійний контроль своїх дій, вчинків та можливостей; дотримуватись вимог конфіденційності; бути впевненим у собі, у своїх силах та можливостях; дотримуватись обережності та прихованості; мати власну систему отримання та аналізу інформації.

Висновки. Введено і обґрунтовано новий клас – систему соціального захисту інформації, який формально перетворює класи захисту інформації в симетричні та функціонально повні відносно вирішуваних задач, а практично забезпечує виконання завдань захисту соціальної та інших видів відкритої інформації на підприємствах та установах будь-якої форми власності, суспільних організаціях та державі в рамках системи національної безпеки та захисту інформаційного простору України. Напрямком подальших досліджень може бути розробка політики та організації систем соціального захисту інформації.

Список літератури

1 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

2 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3 ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

4 ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. Затверджені наказом Держкоммістобудування України від 02.09.96 р. № 156. – С 14.

5 Закон України "Про основи національної безпеки України", від 19.06.2003 № 964-IV.

6 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». В редакції Закону № 2594-IV від 31.05.2005. – С. 5.

7 ПРАВИЛА забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ № 373 від 29.04.06 – С.4.

8 ПОРЯДОК захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Затверджено наказом ДСТСЗІ СБ України № 76 від 24.12 2001. – С. 4.

9 ПОРЯДОК оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Проект ДССЗЗІ від 20.02.2008. – С. 3.

10 Рекомендация МСЭ-Т Е.408. Общая эксплуатация сети. Требования к безопасности сетей электросвязи. – 2004. – С.21;

11 Рекомендация МСЭ-Т Е.409. Общая эксплуатация сети. Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи. – 2004. – С. 16;

12 Панарин И.Н. Информационная война и третий Рим. – М.: (http://top100.km.ru/reader.asp?id=34064&page=1&viewBy=8000&sizechars=150). – 132 с.

13 НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Затверджено наказом № 26 ДСТСЗІ СБ України від 28.05.99. – С. 26.

14 НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. Затверджено наказом № 26 ДСТСЗІ СБ України від 28.05.99. – С. 16.

15 НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Затверджено наказом № 26 ДСТСЗІ СБ України від 28.05.99. – С. 26.

16 ISO/PAS 22399:2007(E). Societal security – Guideline for incident preparedness and

operational continuity management // Firs edition 2007-12-01. – 31 S.

17 Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: МК-Прес, 2005 – 432 с.

18 Кононович В.Г., Тардаскін М.Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування // Захист інформації, № 1, 2006. – 18-30 с.

19 Френцис Фукуяма. Великий крах. Людська природа і відновлення соціального порядку. Пер. З англ. В. Дмитрука. – Львів: Кальварія, 2005. – 380 с.

20 Фукуяма Ф. Наше постчеловеческое будущее. Последствия биотехнологической революции. – М.: АСТ, ЛЮКС, 2004. – 349 с.

21 Калашников М., Русов Р. Сверхчеловек говорит по-русски. Историко-футуристическое расследование. – М.: АСТ. Астрель, 2006. – 639 с.

УДК 519.688

А.В.Шишкин

ЭФФЕКТИВНАЯ СТЕГАНОГРАФИЧЕСКАЯ ПЕРЕДАЧА ИНФОРМАЦИИ В КОЭФФИЦИЕНТАХ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ

Цифровая стеганография в настоящее время применяется в следующих технических задачах: защита информации от несанкционированного копирования путем встраивания цифровых водяных знаков (ЦВЗ) в информационный продукт (звук, изображение, видео); аутентификация информации; мониторинг радиопередач; скрытая передача информации в специальных приложениях и другие. Привлекательность стеганографии состоит в том, что она не требует каких-либо дополнительных ресурсов (объема памяти, расширения объема канала передачи), а использует имеющийся основной (или открытый) канал связи. Вопросам стеганографии посвящены отечественные и зарубежные монографии [1-3].

Совместно с криптографическими методами стеганография позволяет более эффективно решать задачи защиты информации. При этом встроенные ЦВЗ могут обеспечивать свои функции в течение всего времени использования информационного продукта, в то время как однажды взломанная криптосистема утрачивает в дальнейшем свои защитные свойства.

Стеганографическая система характеризуется следующими основными параметрами: вносимыми искажениями (distortions), удельным количеством скрываемой информации (или скоростью) (rate), устойчивостью (robustness) к различного рода помехам – атакам в канале передачи.

Под вносимыми искажениями понимают отличия стегосигнала, т.е. сигнала-носителя с встроенными ЦВЗ от исходного сигнала-носителя (или пустого контейнера). Встраивание ЦВЗ в сигнал-носитель неизбежно приводит к возникновению искажений последнего. В монографии [1] систематизированы всевозможные числовые оценки вносимых искажений. Наиболее распространенной мерой искажений является среднеквадратическая ошибка (СКО).

Удельное количество встроенной информации определяется средним количеством информации на один отсчет сигнала-носителя и измеряется соответственно в бит/отсчет.

Под устойчивостью понимают способность ЦВЗ противостоять различного рода непреодолимым и преднамеренным преобразованиям сигнала (атакам) в канале передачи: аналого-цифровому преобразованию, шумам, операциям сжатия, изменениям масштаба и др.

Указанные параметры – вносимые искажения, количество (скорость), устойчивость – взаимосвязаны. Нельзя одновременно улучшать все три параметра. Исходя из конкретных