УДК 004.056:004.7

С.В. СТАЙКУЦА
Одеська національна академія зв'язку ім.О.С.Попова

ОЦІНКА ІНФОРМАЦІЙНОЇ ТА ФІЗИЧНОЇ БЕЗПЕКИ СИСТЕМИ АНАЛІТИЧНО-ПРОГНОСТИЧНОЇ ІНФОРМАЦІЇ

У статті розглядаються вимоги до інформаційної та фізичної безпеки аналітично-прогностичної (консолідованої) інформації, яка є продуктом діяльності аналітичних та когнітивних центрів, аналізуються загрози, ризики, формуються стратегії системи захисту, основні засоби та заходи захисту. Формулюються відмінності між традиційною інформаційною безпекою «класичної» інформації та інформаційною безпекою консолідованої інформації. Отримані результати дозволяють підвищити ефективність роботи конвергованих систем інформаційної й фізичної безпеки та якість аналітично-прогностичної інформації.

Ключові слова: *інформаційна безпека, фізична безпека, аналітична інформація, консолідована інформація, аналітичні центри, когнітивні центри.*

S.V. STAIKUCA
O.S. Popov Odessa national academy of telecommunications

EVALUATION OF INFORMATION AND PHYSICAL SECURITY OF ANALYTICAL- PROGNOSTIC INFORMATION

The article deals with the requirements for information and physical security analytical and prognostic (consolidated) information that is a product of analytical and cognitive centers are analyzed threats, risks, emerging strategies protection system, fixed assets and protection measures. Formulated differences between traditional information security "classical" information and information security consolidated information. The results allow to increase the efficiency of convergent information systems and physical security and quality of analytical and prognostic information.

Keywords: *information security, physical security, analytical data, consolidated information, analytical centers, cognitive centers.*

Вступ

Інформаційно-аналітичні та когнітивні центри відіграють все більшу роль у діяльності та життєзабезпеченні суспільства у постіндустріальну епоху. Виникли окремі види інтелектуальної діяльності, створена «індустрія» інтелектуальних послуг. Інформаційна безпека консолідованої інформації та інформації, яка здобута методами «законної» конкурентної розвідки, вже набула значного розвитку [1]. Усвідомлено, що повна або часткова відмова від інформаційної безпеки та аналітичної активності може привести до значного підвищення ризиків для бізнесу, суспільству та державі. Проте, проблема оцінки безпеки та ризиків досліджені ще недостатньо.

Значний вклад у вирішення цих проблем внесли: Арутюнян Г., Зайцев Д.Г., Горний М.Б., Дацюк С., Диксон Л., Кроун Крауч, Кузнецов И.И., Стюгін М., Чарльз Хант, Якунін В.І., вітчизняні вчені: Горбатенко В.П., Беата Бель, Бурмагін О., Патора Т., Хоменюк О. та інші. Концептуальні основи інформаційної безпеки представлено в [1]. Спостерігається процес уніфікації та конвергенції систем інформаційної безпеки, систем відеоспостереження та систем фізичної безпеки. Засоби та заходи економічної та інформаційної безпеки консолідованої інформації [2], як продукту інтелектуальної діяльності аналітичних [3] та когнітивних центрів [4], розкриті у [5]. Прикладом оцінки безпеки може служити робота [6], яка проведена відносно системи інформаційного управління держави. Недоліком попередніх робіт можна назвати зведення систем безпеки інформаційних систем до понять «складного об'єкта», «що використовується в теорії управління, та розгляд його трансформації як процесу адаптації в складних системах [6, с. 4]». Сучасні підходи враховують еволюцію систем, самоорганізацію, фрактальні явища [7] та нелінійні ефекти. Тому, питання оцінки безпеки та ризиків у складних конвергованих системах залишаються актуальними.

Цілі та задачі дослідження

Метою даної роботи є аналіз загроз безпеці аналітичної інформації, яка є інтелектуальним продуктом аналітичного та/чи когнітивного центру, розробка стратегії системи захисту, оцінка ризиків реалізації загроз та існуючої системи безпеки інформаційної безпеки.

Інформаційна складова управлінської, виробничої, суспільної, політичної, культурної діяльності набуває небувалої ваги і проходить в умовах як дружньої конкурентної розвідки, так і жорсткого ворожого інформаційного протистояння й інформаційної війни. Консолідована інформація дає можливість приймати управлінські та функціональні рішення для складних систем, що перенавантажені інтенсивними інформаційними потоками «віртуальної реальності».

Основна частина

Коротко дамо формулювання термінів та визначення системи консолідованої інформації, що функціонує в умовах інформаційної війни та прискореної соціальної динаміки.

«Інформаційне управління – це процес вироблення та реалізації управлінських рішень у ситуації, коли управляючий вплив носить неявний характер і об'єкту управління надається (така, що визначається суб'єктом управління) інформація щодо ситуації (інформаційна картина), орієнтуючись на яку цей об'єкт начебто сам обирає лінію своєї поведінки [8, с. 94]». «Інформаційний процес у суспільстві (соціумі)

представляє собою сукупність єдності різноманіття усіляких потоків відтворення, сприймання, оцінки, вироблення, відношення, диспозиції та позиції до інформації та формування на цій основі мотивів соціальної поведінки. Інформаційний процес – це складне переплетення усвідомленого та неусвідомленого впливу джерела інформації на всі рівні людської психіки: від біопсихологічного, до рівня суспільної свідомості. Інформаційний процес може розглядатися: як об'єкт аналітичної роботи; у плані інформаційного впливу на населення …, масову свідомість, інформаційно-психологічної війни; як засіб державного управління. Сукупність різного роду інформаційних процесів, інформаційних систем, системи масової свідомості та психіки складають систему більш складного порядку – інформаційний простір [6, с. 13]». «Консолідована інформація є суспільним знанням, до якого застосований спеціальний відбір, аналіз, оцінка, а також можлива реструктуризація та видозміна з метою придатності для безпосереднього вирішення проблем і задоволення інших інформаційних потреб певних осіб або соціальних груп, які в іншому разі не мали б прямого доступу до цих знань і не могли б ними ефективно скористатись, оскільки вони важко доступні у своїй оригінальній формі й розсіяні по багатьох документах. У такому трактуванні консолідація інформації є складовою інформаційної діяльності, зокрема, таких її видів, як інформаційне забезпечення прийняття рішень [2, с. 7]». Інформаційна безпека виступає як невід'ємна складова частина політичної, економічної, оборонної, екологічної безпеки тощо. «У загальному випадку під інформаційною безпекою розуміється такий стан інформаційного середовища (інформації, інформаційної системи, інформаційного ресурсу) при якому гарантується розвиток цього середовища і її використання в інтересах особистості, суспільства і держави, а також захищеність від будь-яких загроз [5, с. 121]».

Наприклад, для суспільства та особистості є актуальним захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з навмисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи.

З таких позицій ми бачимо, у чому є відмінність інформаційної безпеки, скажімо, інформації у комп'ютерній системі, від інформаційної безпеки консолідованої інформації. Традиційна інформаційна безпека націлена на збереження властивостей інформації: конфіденційності, цілісності та доступності. Необхідною умовою є спостережність інформаційних процесів, інформаційних систем та самої інформації. Головним засобом захисту є створення системи захисту від несанкціонованого доступу з обранням потрібної парадигми захисту [8]. Фактично, традиційна система захисту інформації захищає носії інформації. Інформація може бути захищеною фізично та захищеною від несанкціонованого доступу. Семантика, захист смислів при цьому залишаються поза увагою.

Інформаційна безпека консолідованої інформації стосується, перш за все, змісту та смислу, семантики інформації. Безпека консолідованої інформації повинна мати превентивний і безперервний характер. Система безпеки не може бути відділена від процесу консолідації інформації, а має бути органічно вплетеною в цей процес. Система безпеки не може мати рубіжного характеру і бути зовнішньою підсистемою відносно системи консолідації. Безпека консолідованої інформації має бути сформованою одночасно із формуванням цілей, смислів (семантики) інформації. Зауважимо, що традиційні системи інформаційної безпеки і, тим більше, системи фізичної безпеки, не заперечуються, а навпаки, еволюціонують та вдосконалюються.

Для розробки стратегії системи захисту розробимо модель об'єкту, що захищається. Розглянемо систему, що аналізується в [6], дещо її вдосконаливши: систему контролю масової та індивідуальної свідомості громадян країни. Управління розуміється як «процес організації такого цілеспрямованого впливу на об'єкт, у результаті якого цей об'єкт переводиться у потрібний (цільовий) стан [6, с. 16]». Стан об'єкта змінюється під впливом віртуального (інформаційного простору) та фізичного середовища, а також каналів управління.

Нехай X – стан середовища, з яким взаємодіє об'єкт; Y – стан об'єкта; S – стан оточуючого середовища; U – канал управління, який створюється для реалізації впливу на стан об'єкта управління. Тоді об'єкт можна представити як перетворювач F^0 стану середовищ у стан об'єкта з врахуванням фактора управління

$$Y = F^0(X, U). \tag{1}$$

Якщо під системою управління розуміти «сукупність алгоритмів обробки інформації та засобів їх реалізації, об'єднаних для досягнення заданих цілей управління в об'єкті [6, с. 16], то блок-схема системи управління буде мати вигляд, як на рис. 1.

Тут D_X та D_Y – засоби кваліфікованої оцінки середовища та об'єкта, відповідно. Роль цих засобів виконують аналітичні та когнітивні центри. У якості D_X може виступати інформаційно-аналітичні служби (ІАЦ), які оцінюють особливості сприймання середовища масовою та індивідуальною свідомістю громадян. У якості D_Y можуть виступати когнітивні або прогностичні центри (КЦ), що проводять соціологічний аналіз емпіричних фактів. Інтелектуальним продуктом їх діяльності є консолідована інформація, на основі якої приймаються рішення управління.

$$\begin{cases} X^t = D_X(X) \\ Y^t = D_Y(Y) \end{cases} \tag{2}$$

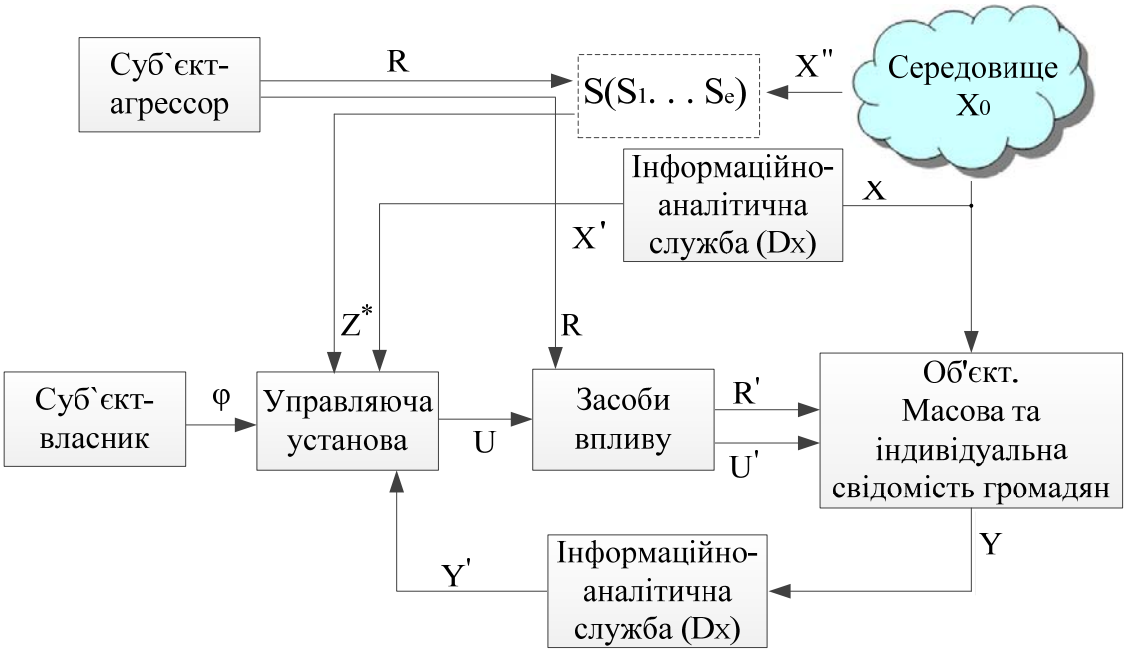

Рис. 1. Система управління масовою та індивідуальною свідомістю громадян

Консолідована інформація поступає на управляючу установу (УУ), яка виробляє команди управління *U*. Ці команди мають бути оброблені виконавчими механізмами (ВК) щоб змінити через вхід управління станом U^t об'єкта. Для функціонування управляючої установи їй повідомляють ціль управління *Z**та задають алгоритм управління $U = \varphi(X^t, Y^t, Z^*)$.

Ціль управління задає суб'єкт, виходячи із свого потрібного майбутнього, тобто деякого певного стану середовища, що йому потрібно і не реалізується без управління. УУ сприймає оточуюче середовище як набір її параметрів

$$S = (s_1 \dots s_n), \tag{3}$$

кожен з яких цікавить суб'єкта і може бути змінений для впливу на стан середовища у потрібну сторону. Будемо вважати, що ситуація, яка сприймається суб'єктом, завжди є такою, що керується:

$$S(U,R) = (s_1(U,R) \dots s_n(U,R)), \tag{4}$$

де *U*, *R* – управління суб'єктів.

Внаслідок складності, нестаціонарності, відсутності можливостей відтворювання експериментів, зашумленості «прогнозування соціальної динаміки практично не має точного математичного апарата [6, с. 16]». Доводиться проводити дослідження логіко-лінгвістичними та евристичними методами класичного аналізу: модель системи, модель загроз, модель користувачів та персоналу, модель захисту, модель системи безпеки.

Перейдемо до аналізу загроз консолідованій інформації. Згідно з [6, с. 21] «захищеність системи управління – це стан системи, за якого відсутні перешкоди, які запобігають УУ перевести об'єкт управління в потрібний (цільовий) стан і які є результатом діяльності суб'єкта-агресора або об'єктивними умовами оточуючого середовища».

Перш за все, як і у будь-якій інформаційній системі, в системі управління масовою та індивідуальною свідомістю громадян мають місце традиційний перелік загроз безпеці інформації. При врахуванні семантики інформації потрібно аналізувати специфічні загрози цільовому функціонуванню системи. Виходячи з моделі інформаційної системи (рис. 1) та визначення захищеності специфічні загрози можна поділити на два види: 1) загрози неадекватної оцінки УУ дійсності (X^t, Y^t, S); 2) загрози порушення процесу управління над об'єктом (*R*, *U*). До першого типу загроз відносяться:

- неадекватне сприймання суб'єктом оточуючого середовища при формуванні простору ситуацій, тобто $X^t \neq X^0$. Наприклад, невірно виконується оцінка економічної, екологічної та політичної ситуації. Це може бути наслідком збоїв у роботі конкурентної розвідки та аналітичних служб;
- формування простору ситуацій {*S*} на основі фальшивої інформації *R*, яка надається агресором;
- некоректна робота оцінювача D_x (службою оцінки особливості сприймання середовища масовою та індивідуальною свідомістю громадян) та видача ним необ'єктивної інформації, тобто $X^t \neq X$;
- некоректна робота оцінювача D_y та видача ним необ'єктивної інформації, тобто $Y^t \neq Y$. В результаті суб'єкт отримує не вірну інформацію щодо реакції об'єкта на управління. Невірні уявлення про громадську думку можуть привести до повної втрати легітимності УУ та переорієнтації на інший суб'єкт. До цього може привести й непрофесійна робота аналітичних та когнітивних центрів.

До другого типу загроз відносяться:

- несприятливі умови оточуючого середовища, які сприймаються об'єктом управління. Технології так званого «кризи-менеджменту» можуть використовуватись для створення та управління

кризовими ситуаціями в інтересах певних суб'єктів;

- існування власної інформаційної інфраструктури суб'єкта-агресора, здатної донести інформацію *R* до об'єкта управління;
- генерування інформаційних потоків *R* суб'єктом-агресором у інформаційних каналах УУ. У цьому випадку класифікація інформаційних потоків U^t та R^t може бути утрудненою, якщо відсутній повний контроль за інформаційними каналами;
- порушення цілісності інформації U^t суб'єктом-агресором. Це може бути спотворення інформації, яка передається УУ, так і розповсюдження інформації суб'єктом-агресором під виглядом УУ;
- вихід із ладу або порушення роботи системи адміністративного управління. Це може бути в наслідок навмисного знищення, техногенної катастрофи або деградації керівного складу.

Розглянемо тезисне модель суб'єкта-агресора та особливості жертв інформаційного впливу. Інформаційний вплив та інформаційна війна пов'язані з реалізацією інтересів суб'єкта. Суб'єкт-агресор, як і система управління (рис. 1), представляє собою мережну інформаційну систему в умовах спільного ресурсу. Він має свої цілі в інформаційному просторі і веде цілеспрямований вплив на систему, що захищається, з метою нанесення їй збитку та отримання переваги у матеріальній сфері. Суб'єкт-агресор здійснює свою діяльність такими етапами: підготовчий етап, етап реалізації загроз безпеці, етап інформаційного впливу на об'єкт.

На підготовчому етапі суб'єкт-агресор проводить атаки, які орієнтовані на збирання інформації щодо роботи системи та стратегії управління. Атаки здійснюються за допомогою перехоплення та аналізу інформаційних потоків, а також іншими технічними та організаційними методами.

На етапі реалізації загроз безпеці суб'єкт-агресор може здійснювати наступні види атак:

- упровадження своїх кадрів в управління, служби, центри, наукові інститути, комунікаційні засоби, які є елементами загальної системи управління, або вербування людей у відповідних структурах;
- отримання суб'єктом-агресором права володіння інформаційними комунікаціями шляхом купівлі інформаційних агентств та підприємств;
- радіоелектронне придушення суб'єктом-агресором інформаційних потоків УУ;
- дезінформація, імітація та демонстративні дії, які вводять противника, тобто УУ, в оману;
- диверсійні акції та спеціальні інформаційні операції;
- застосування економічних та політичних санкцій проти противника;
- порушення роботи апаратних і програмних засобів УУ;
- підміна джерел мовлення УУ: теле-, радіо-мовлення тощо;
- розповсюдження інформації, а також програм, вірусів, червив через Internet;

Етапу реалізації інформаційного впливу на об'єкт може не бути, якщо атака попереднього етапу була цільовою. На цьому етапі можна виділити: дезінформування, маніпулювання, пропаганду.

Інформаційні потоки, які здатні впивати на об'єкт управління (масову та індивідуальну свідомість громадян), за видом психологічного впливу можна поділити на [9]:

- інформаційно-психологічний вплив (інформаційно-пропагандистський). Ставить своєю метою формування певних соціальних ідей, поглядів, уявлень, переконань;
- психогенний вплив. Являється наслідком шокового впливу оточуючих умов або яких-небудь подій не свідомість людини, в результаті чого вона не в змозі раціонально діяти, втрачає орієнтацію у просторі, почуває афект або депресію, впадає у паніку, ступор тощо. Використовуються для генерації неадекватного страху перед якою-небудь загрозою;
- психоаналітичний чи психокорекцій ний вплив. Вплив на свідомість терапевтичними засобами, які виключають свідомий опір як окремих індивідів так і групи людей у не сонному стані. Це досягається, наприклад, при швидкому надходженні різних слів, образів, фраз;
- нейролінгвістичне програмування (НЛП). Змінювання мотивації людей шляхом введення у їх свідомість спеціальних лінгвістичних програм;
- психотропний (екстрасенсорний) вплив. Здійснюється шляхом передавання інформації через позапочуттєве (неусвідомлене) сприймання. Застосовуються генератори високочастотного та низькочастотного кодування мозку, біолокаційних установок, по використанню хімічних та біологічних засобів з метою стимулювання певних психологічних реакцій. "Наприклад, використовується ефект, що викликається кольоровими плямами, вбудованими у комп'ютерний вірус. … Цей вірус здатен негативно впливати на психофізіологічний стан користувача персонального комп'ютера (можливий навіть летальний випадок). Принцип його дії заснований на ефекті 25-го кадру, який, можливо, є потужним засобом напучення [6, с. 16]".

Ведення інформаційного протиборства суб'єктом-агресором здійснюється за принципами:

- використання принципу інформаційної асиметрії, трансформації структури інформаційного простору з метою створення та маскування у його інформаційних об'єктах нових, асиметричних властивостей, вразливих для асиметричної зброї;
- прихованість та анонімність оперування інформаційно-психологічними впливами, можливість проводити їх «під чужим прапором» і з будь-якої точки інформаційного простору;
- плавність переключення інформаційних впливів, інтенсивність та тривалість яких регулюється у широких межах: від організації інформаційних «ударів», «вкидів», «блокад», до розтягнутих на роки мікродозованих впливів;
- багатоаспектність та багатооб'єктність впливу з високим ступенем координації у часі та просторі.

Проникнення інформаційних систем та технологій в усі сфери життя суспільства дає змогу будувати інформаційний вплив за будь-яким, коригованим у часі, алгоритмом впливу на різні сфери, процеси, об'єкти, групи, персони тощо у потрібній послідовності. Це дозволяє оптимізувати отримання кінцевого результату та витрати на його досягнення. Також можливе попереднє моделювання, перегляд варіантів;

- здатність малими інформаційними впливами отримати великі кінцеві результати. Завдяки високому рівню моделювання розвитку ситуацій, який дає можливість виявляти тенденції та управляти при моделюванні попередніми змінами ситуації, стає можливим внесення у процесі інформаційно-психологічної війни вплив з малими витратами «енергетики» у випереджаючому режимі;
- перенесення функцій стримування на інформаційну сферу. Досягнення інформаційного домінування створює базу та необхідні умови на превентивність дій в реалізації функцій стримування. Інформаційне домінування може стати головним механізмом стримування;
- інформатизація як головний резерв підвищення ефективності силових (військових) операцій. Вартість традиційних систем озброєнь має практичну межу, яка вже досягнута багатьма країнами;
- наведення хаосу у сфері, що піддається інформаційному впливу, та наступне управління хаосом (або за допомогою хаосу) може стати одним із принципів отримання потрібних результатів.

Перейдемо до опису моделі користувачів (людського фактору) та ризиків безпеки за усіма факторами. Джерелом ризику можуть бути такі фактори або їх сукупності: людський фактор; технічний, точніше програмно-апаратний фактор та фактори середовища. Значення ризику залежить від потенційної ймовірності реалізації загрози, та тягаря можливих наслідків.

Розглянемо модель користувачів і персоналу. Людський фактор порушує стан захищеності системи внаслідок неадекватної діяльності персоналу, яка може бути результатом: неможливості виконання людиною доручених йому робіт внаслідок перенавантаження; навмисні дії співробітника, які порушують правила функціонування системи і які можуть бути наслідком адаптації людини до середовища або його переконань; некомпетентність співробітника. Ризик від людського фактору можна виразити формулою [6, с. 31]

$$R_M \propto k(N_0 - N)\left[\sum_{n=1}^{N}(p_n \cdot v_n) + 1\right], \tag{5}$$

де k – коефіцієнт важливості організаційної структури; N_0 – мінімально необхідна кількість працівників, необхідних для реалізації організацією своїх функцій; N – кількість працівників; p_n – ймовірність неадекватної поведінки персоналу (залежить від якості підбору персоналу, виховної роботи, організаційно правових заходів, частості інцидентів тощо); v_n – важливість даної посади людини за можливості впливу на процеси в організації, та рівень інформованості щодо процесів організації.

Ризик від технічних (програмно-апаратних) факторів пропорційний величині

$$R_T \propto k\left[\sum_{j=1}^{N}\left(p_j \cdot v_j\right)\right], \tag{6}$$

де k – коефіцієнт важливості організаційної структури; N – загальна кількість автоматизованих систем (АС); p_j – ймовірність реалізації несанкціонованого доступу до АС, яка залежить від міцності захисту, ймовірності відмови обладнання тощо ; v_j – важливість АС у загальній організаційній структурі за кількістю інформації, що обробляється та її значимості.

У формулах (5) і (6) замість знака рівності стоїть знак пропорційності. Формули відображають не кількісні а якісні залежності у зв'язку з відсутністю вхідних даних, статистики інцидентів, кадрового складу тощо.

Що стосується залежності ризиків від факторів середовища, то у роботі [6, с. 33] з'ясовується наступне. У складних системах, які складаються із великого числа елементів або характеризуються складною поведінкою, мають місце нелінійні закони. Наприклад, у людини більшість її сенсорів (зору, слуху, тактильні) виробляють реакцію, яка пропорційна логарифму інтенсивності подразнення. Найпростішими нелінійними законами є показникові закони. Тому запропоновано величину ризику від факторів середовища оцінювати формулою

$$R_C \propto S^{\left[\frac{\langle f_E \cdot f_{inf}\rangle_{\text{агресор}}}{\langle f_E \cdot f_{inf}\rangle_{\text{УУ}}}\right]}, \tag{7}$$

де f_E – економічні показники середовища; f_{inf} – показники об'єму інформаційної інфраструктури; кутові дужки показують усереднені показники; відношення у показнику степеня є величина переваги показників суб'єкта-агресора над показниками УУ; S – знаходиться дослідним шляхом. Як правило, $S \geq e$.

Розглянемо тепер сумарний ризик від усіх типів і видів загроз. Результатом реалізації будь-якої загрози є генерація інформаційного (комунікаційного) потоку. Ризик генерації шкідливого потоку у тій же роботі визначається як

$$R_C \propto S^{\left[\frac{\langle f_E \cdot f_{inf}\rangle_{\text{агресор}}}{\langle f_E \cdot f_{inf}\rangle_{\text{УУ}}}\right]}, \tag{8}$$

де N – кількість комунікаторів; D_i – ступінь довіри до джерела з урахуванням як усвідомленої довіри так і довіри внаслідок психологічного впливу; O_i – кількість людей, що сприймають даний комунікаційний потік; p_i – ймовірність генерації суб'єктом-агресором інформаційного потоку у даному комунікаційному пристрої.

Ризики визначають інтенсивність успішних атак на систему. Величина p_i у формулі (8) створюється сукупністю всіх розглянутих факторів із врахуванням також законодавчих та організаційних заходів і описується формулою [6, с. 34].

$$p_i = 1 - \frac{1}{e^{q(R_{Mi}+R_{Ti}+R_{Ci}+R_{Zi})}}, \quad (9)$$

де R_{Zi} – показник ризику від фактору законодавчих або організаційних заходів; q – коефіцієнт, який визначається емпірично.

Експоненціальна форма закону (9) визначає швидкість розповсюдження збурень у хаотичних фрактальних системах і може бути застосована для людського суспільства [10].

Висновки

У даній статті проаналізовані загрози безпеці аналітичної інформації, яка є інтелектуальним продуктом аналітичних та/чи когнітивних центрів, розроблена стратегія системи захисту, проведена інтерпретація відомих законів про оцінку ризиків реалізації загроз та існуючої системи безпеки інформаційної безпеки. Сформульовані відмінності між традиційною інформаційною безпекою інформації та інформаційною безпекою консолідованої інформації. Отримані результати дозволяють підвищити ефективність роботи конвергованих систем інформаційної та фізичної безпеки та якість аналітично-прогностичної інформації. Перевірка адекватності моделей розрахунку ризиків на основі експериментальної статистики й розробка прогнозу є метою подальшої роботи.

Література

1. Жук Е.И. Концептуальные основы информационной безопасности /Е.И. Жук // Электронное научно-техническое издание. – М.: Издатель ФГБОУ ВПО «МГТУ им. Н.Э. Баумана». Эл. № ФС 77 – 48211, 2010. – 38 с. – Режим доступа: technomag.bmstu.ru/doc/143237.html.

2. Матвієнко О.В. Консолідована інформація : навч. посібник / О.В. Матвієнко, М.Н. Цивін. – К.: «Центр учбової літератури», 2014. – 134 с.

3. Аналитические центры в политике, экономике, бизнесе / Київ, 2014. – 70 с.

4. Когнитивные центры как информационные системы для стратегического прогнозирования /Десятов И.В. и др. // Препринт ИПМ им. М.В. Келдыша № 50, Москва, 2010. – 28 с. Режим доступа: http://keldysh.ru/papers/2010/source/prep2010_50.pdf

5. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.

6. Стюгин М. Оценка безопасности системы информационного управления Российской Федерации. – Режим доступа: http://psyfactor.org/lib/styugin4.htm

7. Скопцов В.В. Социальный фрактал как фактор минимизации уровня неопределенности в социуме. / В.В. Скопцов. – 2011. – 6 с. – Режим доступа: http://maxpark.com/user/733577252/content/681572.

8. Манойло А.В. Государственная информационная политика в особых условиях: Монография. – М.: МИФИ, 2003. – 388 с.

9. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) – Мн.: Харвест, 1999. – 363 с. – Режим доступа: http://www.evartist.narod.ru/text19/001.htm.

10. Ситникова Д.Л. Самоорганизация и власть идеи / Д.Л. Ситникова // 4-й Всероссийский постоянно действующий научный семинар «Самоорганизация устойчивых целостностей в природе и обществе». – Томск.: Издатель ТУСУРЭ, 2000. – 6 с. – Режим доступа: http://vasilievaa.narod.ru/gu/mat_conf/SOV/SOV46.htm.

References

1. Zhuk E.I. Kontseptual'nye osnovy informatsionnoy bezopasnosti / Zhuk E.I. // Elektronnoe nauchno-tekhnicheskoe izdanie. – M.: Izdatel' FGBOU VPO «MGTU im. N.E. Baumana». El. № FS 77 – 48211, 2010. – 38 s. – Rezhim dostupa: technomag.bmstu.ru/doc/143237.html.

2. Matvієnko O.V. Konsolidovana informatsiya : navch. posibnik / O.V. Matvієnko, M.N. Tsivin. – K.: «Tsentr uchbovoї literaturi», 2014. – 134 s.

3. Analiticheskie tsentry v politike, ekonomike, biznese / Kiïv, 2014. – 70 s.

4. Kognitivnye tsentry kak informatsionnye sistemy dlya strategicheskogo prognozirovaniya /Desyatov I.V. i dr. // Preprint IPM im. M.V. Keldysha № 50, Moskva, 2010. – 28 s. Rezhim dostupa: http://keldysh.ru/papers/2010/source/prep2010_50.pdf

5. Kavun S. V. Ekonomichna ta informatsiyna bezpeka pidpriєmstv u sistemi konsolidovanoї informatsiї : navchal'niy posibnik / S. V. Kavun, A. A. Pilipenko, D. O. Ripka. – Kh. : Vid. KhNEU, 2013. – 364 s.

6. Styugin M. Otsenka bezopasnosti sistemy informatsionnogo upravleniya Rossiyskoy Federatsii. – Rezhim dostupa: http://psyfactor.org/lib/styugin4.htm

7. Skoptsov V.V. Sotsial'nyy fraktal kak faktor minimizatsii urovnya neopredelennosti v sotsiume. / V.V. Skoptsov. – 2011. – 6 s. – Rezhim dostupa: http://maxpark.com/user/733577252/content/681572.

8. Manoylo A.V. Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh: Monografiya. – M.: MIFI, 2003. – 388 s.

9. Krys'ko V.G. Sekrety psikhologicheskoy voyny (tseli, zadachi, metody, formy, opyt) – Mn.: Kharvest, 1999. – 363 s. – Rezhim dostupa: http://www.evartist.narod.ru/text19/001.htm.

10. Sitnikova D.L. Samoorganizatsiya i vlast' idei / D.L. Sitnikova // 4-y Vserossiyskiy postoyanno deystvuyushchiy nauchnyy seminar «Samoorganizatsiya ustoychivykh tselostnostey v prirode i obshchestve». – Tomsk.: Izdatel' TUSURE, 2000. – 6 s. – Rezhim dostupa: http://vasilievaa.narod.ru

Рецензія/Peer review : 21.12.2014 р. Надрукована/Printed :2.1.2015 р.