УДК 354.42

О.В. Левченко

Міністерство оборони України, Київ

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО КОМПЛЕКСНОЇ ОЦІНКИ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На основі концептуального підходу до комплексної оцінки стану інформаційної безпеки визначено узагальнені критерії і показники рівня інформаційної безпеки.

Ключові слова: *інформаційні технології, інформаційна безпека, критерії та показники рівня інформаційної безпеки.*

Вступ

Постановка проблеми. Аналіз літератури. Однією з основних тенденцій розвитку воєнно-політичної обстановки у світі є прискорення розвитку інформаційних технологій, збільшення спроможностей держав щодо проведення інформаційних операцій, а також посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань у воєнних конфліктах.

Сьогодні світовий геополітичний простір та внутрішньодержавні відносини формуються в умовах інформаційного протиборства. Для нашої держави ця проблема є особливо актуальною. Зважаючи на агресивні дії Російської Федерації, остаточну невизначеність геополітичного статусу, політичну нестабільність, нестійкість вітчизняного інформаційного простору, Україна останнім часом перебуває під надпотужним інформаційним тиском.

В умовах збройної агресії Росії проти України, а саме анексії Криму, підбурювання, організації та всебічного забезпечення збройного протистояння на Сході нашої держави, проявляється нова тенденція ведення Росією воєнних дій – так званої "гібридної війни".

Відомий американський військовий теоретик Френк Хоффман одним з перших зазначив: "…війни сучасної епохи характеризує процес гібридизації, у рамках якого змішуються традиційні форми війни, кібервійни, організованої злочинності, іррегулярних конфліктів, тероризму тощо" [1]. Щоб охарактеризувати нову військову реальність, саме він запропонував термін "гібридна війна", що дає змогу найбільш точно відобразити важливі зміни в характері воєн при збереженні їх незмінної природи. Така війна виходить за рамки традиційних понять про неї, вона набуває комбінованого характеру, перетворюючись у клубок політичних інтриг, запеклої боротьби за політико-економічне домінування над країною-супротивником, за території, ресурси й фінансові потоки.

Водночас усе це супроводжується цілеспрямованими інформаційними заходами. В епоху інтенсивного розвитку інформаційних технологій, наявності глобальних інформаційних мереж і не менш глобалізованих засобів масової інформації складова "інформаційного супроводу" у гібридних війнах має надзвичайно важливе, якщо не вирішальне, значення.

За цілою низкою ознак можна стверджувати, що ключова роль у війні Росії проти України належить інформаційній складовій у формі надпотужної інформаційної кампанії щодо провокування розколу в українському суспільстві та забезпечення встановлення контролю над південно-східними регіонами України. В цих умовах гостро постає проблема захисту національного інформаційного простору від зовнішніх інформаційних загроз.

Вирішення цієї проблеми полягає не лише у виявленні і протидії цим загрозам, а й у наявності дієвих механізмів всебічної комплексної оцінки стану інформаційної безпеки держави, які у підсумку дозволять своєчасно організовувати боротьбу із зазначеними загрозами.

Дослідженню в цій галузі присвячено низку робіт, у яких пропонуються різні підходи до комплексної оцінки рівня інформаційної безпеки. Так, наприклад, у [2] викладено системний підхід до побудови комплексного захисту інформаційної системи підприємства та описано методику побудови такої системи із застосуванням технічних і криптографічних засобів захисту. У [3] розглянуті принципи й методи аудита інформаційної безпеки на основі процесорного підходу, наведено певні методи оцінювання.

Найбільш системно до вирішення завдань безпеки, на наш погляд, підійшов у своїх роботах В. В. Домарєв. Ним запропоновано тривимірну модель, що містить основні етапи, напрямки та методи забезпечення безпеки різних систем [4]. Визначено, що специфічними особливостями завдання створення систем захисту є:

неповнота й невизначеність вихідної інформації про склад і характер загроз;

багатокритеріальність завдання, що пов'язано з необхідністю врахування великої кількості часткових показників;

наявність кількісних і якісних показників, які необхідно враховувати під час вирішення завдань розроблення та впровадження систем захисту та протидії;

неможливість застосування класичних методів оптимізації.

Враховуючи викладене, пошук шляхів комплексної оцінки стану інформаційної безпеки держави є актуальним науковим і практичним завданням.

Метою статті є розроблення концептуального підходу до комплексної оцінки рівня інформаційної безпеки та визначення його узагальнених критеріїв і показників.

Основний матеріал

Діяльність щодо забезпечення безпеки виникає в ході вирішення протиріччя між небезпекою і потребою управляти безпекою: передбачати, запобігати, локалізувати й усувати збиток від впливу небезпеки [5].

Оцінка рівня безпеки завжди відносна. Спроби безпосередньо приписати цій оцінці чисельне значення в більшості випадків безперспективні в плані подальшої інтерпретації результатів.

Безпека – поняття комплексне, а тому не може розглядатися як проста сума складових її частин. Ці частини взаємопов'язані та взаємозалежні. Крім того, кожна частина є критично значущою та має різний ступінь впливу на величину узагальненого критерію.

Отже, методи, що передбачають осереднення часткових критеріїв безпеки (нехай і неявне) при комплексному оцінюванні стану безпеки, неприйнятні.

Часткові критерії та показники, що використовуються для оцінювання стану підсистем безпеки, зазвичай, носять суперечливий характер. Це призводить до того, що завдання комплексного оцінювання стану інформаційної безпеки є багатокритеріальним.

Для розв'язання багатокритеріальних задач, зазвичай, використовуються різні методи згортки критеріїв в один узагальнений (інтегральний) критерій. Найбільш простий метод визначення інтегрального критерію полягає у виділенні одного з критеріїв як основного, а всі інші критерії додаються до обмежень, у яких задається область припустимих значень вектора незалежних змінних. Таким чином завдання прийняття рішення з векторним критерієм зводяться до завдань зі скалярним аргументом.

Основний недолік такого підходу полягає в тому, що оцінювання стану інформаційної безпеки фактично ведеться лише за одним критерієм. Значення інших критеріїв, якщо вони задовольняють обмеження, не впливають на результати оцінювання.

Отже, враховуючи багатовимірюваність безпеки, спроба оцінити її рівень за одним параметром (наприклад, який має стандартний кількісний вираз) не є коректною. Тому такий спосіб отримання згортки розв'язання завдань, пов'язаних з оцінкою стану безпеки, є неприйнятним.

Як і кожний вид безпеки, інформаційна безпека не існує сама по собі. Вона забезпечується для людини і нею ж оцінюється. Тому поняття інформаційної безпеки має не тільки об'єктивну, але й суб'єктивну сторону, оскільки її рівень оцінюється в остаточному підсумку людиною. Це досить важливий аспект: суб'єктивність в оцінюванні рівня інформаційної безпеки, з одного боку, призводить до необхідності оперування лінгвістичними змінними (основними структурними одиницями у мові людей) і, як наслідок, до необхідності застосування апарату евристичної логіки, а з іншого боку – до того, що у шкалі оцінок рівня безпеки може з'являтися діапазон ‘‘умовної прийнятності’’ [6].

Припустимо, що рівень інформаційної безпеки оцінюється від нуля до одиниці. При цьому нулю відповідає абсолютно неприйнятний рівень безпеки (нижча оцінка), а одиниці – повністю задовольняючий рівень (найвища оцінка).

При оцінюванні окремих сторін безпеки системи існує деякий граничний рівень, вище якого система вважається безпечною, а нижче – ні. Рівень залишкових ризиків при цьому лише зрушує граничне значення в той чи інший бік, не змінюючи картину в цілому.

Під час комплексного оцінювання стану інформаційної безпеки ситуація якісно змінюється. Певні ризики, неприйнятні за одних обставин, при інших оцінюються як припустимі. Причому, такими обставинами, які впливають на оцінювання стану безпеки, можна назвати і наявність або відсутність інших ризиків.

Будь-які неконтрольовані зовнішні або внутрішні процеси потенційно можуть призвести до виникнення загроз. Реалізація цих загроз спричиняє різні деструктивні процеси, що, у свою чергу, впливає на стан безпеки всієї системи. Порушення нормального функціонування системи знаходить своє відбиття в значеннях критеріїв і показників, які використовуються для оцінки стану її безпеки [7]. Це, у свою чергу, свідчить про необхідність виваженого вибору узагальнених критеріїв і показників стану інформаційної безпеки. У концептуальному плані підхід до вибору зазначених критеріїв і показників має бути уніфікованим.

Іншими методами визначення комплексного критерію є адитивна та мультиплікативна згортка.

Адитивний критерій є найбільш простим. Водночас, унаслідок можливості необмеженої компенсації значень одних критеріїв за рахунок інших, він є нечутливим до крайніх значень окремих критеріїв.

Отже, методи, в основі яких лежить припущення про лінійне поводження системи (адитивна згор-

тка припускає саме таку модель), при комплексному оцінюванні рівня інформаційної безпеки зазвичай не можуть адекватно відображати реальну ситуацію. Тому адитивна згортка для комплексного оцінювання рівня безпеки, у більшості випадків, також є неприйнятною.

Значення мультиплікативного критерію, на відміну від адитивного, різко зменшується при малих значеннях окремих критеріїв. Це дає змогу підвищити чутливість узагальненого критерію до незначних змін його складових.

Таким чином, для завдань, пов'язаних із забезпеченням інформаційної безпеки, у більшості випадків, найбільш доцільним вважається застосування мультиплікативної згортки векторного критерію:

$$K = \prod_i (K_i)^{S_i}, \qquad (1)$$

де K_i – часткові критерії; S_i – вага часткового критерію K_i (ступінь впливу на узагальнений критерій), яка визначається експертним шляхом.

При виконанні згортки з метою уніфікації різнорідних критеріїв використовують перехід від абсолютних значень критеріїв до відносних величин. Для цього фіксується шкала можливих значень для критеріїв і можливі межі зміни для кожного з них. Наприклад, якщо за шкалу прийняти інтервал [0; 1], а межі зміни критерію K_i знаходяться між K_i^{min} та K_i^{max}, то у якості відносного значення критерію буде виступати величина:

$$\hat{K} = \frac{K_i - K_i^{min}}{K_i^{max} - K_i^{min}}. \qquad (2)$$

Однак, подекуди отримання від особи, що приймає рішення (ОПР), надійної кількісної інформації для побудови K буває ускладненим. У таких випадках прагнуть одержати від ОПР, в основному, тільки якісну інформацію. Наприклад, про те, який із критеріїв найбільш або найменш значущий, який з критеріїв може бути погіршений, а для яких погіршення є вкрай небажаним тощо.

Отримання такої інформації може здійснюватись за алгоритмом Беленсона–Капура [7].

Певні фактори, що стосуються інформаційної безпеки, можуть взагалі не підлягати кількісному виміру. В такому разі під час їхнього оцінювання застосовують штучні прийоми. Наприклад, кожному фактору зіставляється кількісна бальна шкала [8]. Приклад такої шкали наведено в табл. 1.

Таблиця 1

Оцінювальні шкали для визначення значущості факторів

Перелік питань, що дають змогу виділити значущість факторів	Пояснення значення шкал
1	2
Як довго цей фактор буде впливати на інформаційну безпеку держави (шкала №1)	**Недовго (0,3).** Цей фактор буде здійснювати нетривалий вплив на інформаційну безпеку держави і за певних умов та припущень його можна звести до мінімуму.
	Тривало (0,5). Цей фактор протягом значного відрізку часу буде здійснювати вплив на інформаційну безпеку держави і може зі збігом обставин продовжувати або скорочувати свою дію.
	Довго (0,7). Цей фактор буде впливати на інформаційну безпеку держави, не зважаючи на зміни, які пов'язані зі значними організаційними, технічними, економічними перетвореннями.
До яких наслідків для оцінювання інформаційної безпеки держави може призвести нехтування цим фактором (шкала №2)	**Незначні (0,3).** Нехтування цим фактором (його неврахування) не має відчутного впливу на оцінювання інформаційної безпеки держави.
	Відчутні (0,5). Нехтування цим фактором призводить до більш відчутного впливу на оцінювання інформаційної безпеки держави, але ці зміни можуть бути компенсовані урахуванням інших факторів, або іншим шляхом за незначний проміжок часу..
	Значні (0,7). Нехтування цим фактором призводить до значного впливу на інформаційну безпеку держави і матиме руйнівні наслідки на існуючому етапі розвитку держави. Зміни, пов'язані з нехтуванням цього фактору можуть бути усунені тільки протягом значного відрізку часу із залученням значних ресурсів.
	Катастрофічні (0,9). Нехтування цим фактором призводить до настільки значного впливу на інформаційну безпеку держави, що наслідки цих змін неможливо усунути у найближчому майбутньому та виникне проблема з їх усуненням у подальшому.
Який зворотний вплив здійснює система інформаційної безпеки на цей фактор (шкала №3)	**Не здійснює (0,1).** Система інформаційної безпеки не здійснює ніякого впливу на фактор, що розглядається.
	Має слабкий вплив (0,3). Зі зміною системи інформаційної безпеки держави цей фактор змінюється незначним чином і за певних припущень може розглядатися як самостійний.
	Значно впливає (0,5). Зі зміною системи інформаційної безпеки цей фактор може змінитися таким чином, що він частково увійде до більш глобального або значно зросте його вплив.
Ступінь зв'язку між цим фактором і рештою факторів (шкала №4)	**Віддалено пов'язані (0,3)**. Цей фактор пов'язаний з іншим фактором таким чином, що їх вплив один на одного не призводить до відчутних змін системи інформаційної безпеки держави.

Закінчення табл. 1

1	2
	Сильно пов'язані (0,7). Цей фактор пов'язаний із співставленим таким чином, що їхній взаємний вплив призводить до суттєвих змін в системі інформаційної безпеки держави і не може бути знехтуваний без наслідків для оцінювання.
	Пов'язані визначальним чином (0,9). Цей фактор пов'язаний із співставленим таким чином, що їхній взаємний вплив може позначитися на системі інформаційної безпеки держави значним чином і не може змінитися навіть з плином часу.

Зважаючи на вищевикладене, експертові бажано запропонувати методику, за якою він має призначити бали та в подальшому оцінити стан інформаційної безпеки. Вона може складатись із таких етапів [9].

1. Експертне оцінювання факторів, що впливають на стан інформаційної безпеки за шкалами, наведеними у таблиці.

2. Визначення часткових показників інформаційної безпеки та їх вагу.

3. Визначення мінімального та максимального значень відповідного показника.

4. Обчислення відносного значення критерію за формулою (2).

Таким чином, запропонований підхід дає змогу комплексно оцінювати рівень інформаційної безпеки, що підвищить ступінь обґрунтованості прийняття відповідних рішень.

Висновки

Забезпечення інформаційної безпеки носить комплексний характер, ґрунтується на логіко-евристичному аналізі можливих негативних наслідків, а багато факторів, що впливають на її рівень можуть взагалі не підлягати кількісному виміру. Запропонований підхід до визначення критеріїв інформаційної безпеки дає змогу уникнути труднощів, пов'язаних із оцінюванням її рівня.

Подальші дослідження доцільно проводити за такими напрямками:

– розроблення методів моніторингу рівня інформаційної безпеки, що дадуть змогу не лише контролювати, а й підтримувати такий стан інформаційної безпеки, за якого її показники перебуватимуть у допустимих межах;

– визначення взаємозв'язків відносних показників рівня інформаційної безпеки за всіма її сферами;

– обґрунтування нормуючих вагових коефіцієнтів для оцінювання стану інформаційної безпеки в цілому.

Список літератури

1. Frank G. Hoffman. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Confict. "Strategic Forum", Institute for National Strategic Studies National Defense University. No. 240. April 2009 [Електронний ресурс]. – Режим доступу: http://www.ndu.edu/inss.

2. Садердинов А.А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. / А.А. Садердинов, В.А. Трайнев, А.А. Федулов – М.: Дашков К°, 2005. – 336 с.

3. Курило А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиров, В.Б. Голованов. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: Диасофт, 2004. – 992 с.

5. Ажмухамедов И.М. Концептуальная модель управления комплексной безопасностью системы / И.М. Ажмухамедов // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика". – 2010. – № 1. – С. 62-66.

6. Белов П.Г. Теоретические основы системной инженерии безопасности / П.Г. Белов. – К.: КМУ ГА, 2006.

7. Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, Ф.Г. Гурвич. – М.: Статистика. 1980. – 264 с.

8. Саати Т. Аналитическое планирование / Т. Саати, К. Кернс. – М., Радио и связь, 1991.

9. Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок. – Ін-т пробл. нац. безпеки.– К.: Інтертехнологія, 2009. – 136 с.

Надійшла до редколегії 11.08.2015

Рецензент: д-р техн. наук проф. К.С. Васюта, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К КОМПЛЕКСНОЙ ОЦЕНКЕ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Левченко

На основе концептуального похода к комплексной оценке состояния информационной безопасности установлены обобщенные критерии и показатели информационной безопасности.

Ключевые слова: *информационные технологии, информационная безопасность, критерии и показатели информационной безопасности.*

THE CONCEPTUAL APPROACH OF ASSESSING THE STATE OF INFORMATION SECURITY

O.V. Levchenko

It is set on the basis of conceptual analysis of concept of complex informative security generalized criteria and indexes of informative security.

Keywords*: information technologies, informative security, criteria and indexes of informative security.*