УДК 340.13

ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент, професор РАЕ*

ІНФОРМАЦІЙНА БЕЗПЕКА: ІНДИКАТОРИ [*]

Анотація. *Дослідження індикаторів інформаційної безпеки як основного показника її стану.*

Ключові слова: *індикатор, інформаційна безпека, комп’ютерна злочинність, комп’ютерний тероризм, властивість інформації.*

Аннотация. *Исследование индикаторов информационной безопасности как основного показателя её состояния.*

Ключевые слова: *индикатор, информационная безопасность, компьютерная преступность, компьютерный терроризм, свойства информации.*

Summary. *Research of indicators of informational safety as basic index of its state.*

Keywords: *indicator, informational safety, computer-related crime, computer terrorism, properties of information.*

Постановка проблеми. Доктрина інформаційної безпеки України [2] вирізняє такі життєво важливі інтереси в інформаційній сфері:

1) особи:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;

– захищеність від негативного інформаційно-психологічного впливу;

2) суспільства:

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди;

– формування і розвиток демократичних інститутів громадянського суспільства;

3) держави:

– недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;

– побудова та розвиток інформаційного суспільства;

– забезпечення економічного та науково-технологічного розвитку України;

– формування позитивного іміджу України;

– інтеграція України у світовий інформаційний простір.

[*] Індикатор – (мова оригіналу): 1) доступная наблюдению и измерению характеристика изучаемого объекта, позволяющая судить о других его характеристиках, недоступных непосредственному исследованию; 2) визуальный указатель хода процесса или состояния объекта [1].

Дослідженнями [3 – 4] також було встановлено наступне.

По-перше. У переважній більшості чинних законодавчих та інших нормативно-правових актів, які спрямовані на встановлення, розвиток та регулювання інформаційних відносин, не застосовується поняття “інформаційна безпека”.

По-друге. Переважна більшість положень законів України та інших нормативно-правових актів, які мають безпосереднє відношення до інформаційних відносин, мають спрямованість саме на захист інформації.

По-третє. Об’єктами інформаційних відносин є інформація, норми і правила, які визначають ці відносини, а також людина, суспільство, держава, а суб`єктами – держава, суспільство, людина, норми і правила, які визначають ці відносини.

По-четверте. Об’єктами інформаційної безпеки є інформація у всіх її проявах, джерела інформації, механізми та засоби її створення, доступу і розповсюдження та наслідки її використання, а також установчі і регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають процеси і процедури формування, використання та припинення дії цих механізмів та засобів, людина, суспільство та держава, а суб’єктами – людина, суспільство, держава.

По-п’яте. Об`єктом захисту інформації є інформація, а суб’єктами – дії з інформацією на всіх стадіях її “життєвого циклу” (створення, розповсюдження, збереження, знищення, спотворення, фальсифікація та ін.).

Стратегія національної безпеки України [5] серед механізмів реалізації державної політики національної безпеки передбачає удосконалення системи управління національною безпекою шляхом, зокрема, *розробки та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів),* що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці. І це є абсолютно вірним та логічним напрямом максимально наближеної до реальності оцінки стану національної безпеки.

Не викликає сумніву у вірності та коректності й твердження “Доктрини інформаційної безпеки України” [2], що *“інформаційна безпека є невід’ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.”*

Таким чином виникає питання розробки системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень національної інформаційної безпеки.

Метою статті є – на основі сутності та визначення поняття “інформаційна безпека”, а також законодавчо визначених реальних та можливих (потенційних) загроз у сфері забезпечення інформаційної безпеки, окреслення методологічного підходу до означення індикаторів, які у сукупності, визначають, у певному масштабі часу, стан національної системи інформаційної безпеки як в цілому, так і в будь-якій сфері національної безпеки, складовою якої вона є.

Виклад основних положень. Таким чином, виникає питання розробки системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень національної інформаційної безпеки.

В дослідженнях, які були присвячені питанням сутності та визначення понять “інформаційна безпека” та “безпека інформації” [4], показано, що до властивостей інформаційної безпеки, насамперед, відносяться: повнота, вчасність, вірогідність,

санкціонованість розповсюдження, конфіденційність, цілісність та доступність інформації, а також відсутність її негативного впливу.

З методологічної точки зору, саме ці властивості, на погляд автора, повинні бути базовими під час визначення індикаторів, що характеризують рівень інформаційної безпеки.

Цю тезу підтверджують законодавчо закріплені наступні реальні та потенційні загрози національній безпеці в інформаційній сфері, сфері інформаційної безпеки.

Так Закон України “Про основи національної безпеки” [6, ст. 7)] визначає основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційної сфері:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп’ютерна злочинність та комп’ютерний тероризм;

– 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.

Фактично в унісон з наведеними загрозами в інформаційної сфері, Доктрина інформаційної безпеки України [2] визначає наступні основні реальні та потенційні загрози інформаційній безпеці України:

1) у зовнішньополітичній сфері:

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

зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

2) у сфері державної безпеки:

негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

3) у воєнній сфері:

інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

поширення суб’єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) у соціальній та гуманітарній сферах:

недодержання прав людини і громадянина на одержання інформації, необхідної для захисту їх соціально-економічних прав;

поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності;

тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;

послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;

відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинутих держав;

6) в екологічній сфері:

приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру.

Як ми бачимо, головний сенс всіх перелічених загроз знаходиться у площині повноти, вчасності, вірогідності, конфіденційності та цілісності інформації з одночасним забезпеченням її доступності за умови санкціонованості розповсюдження інформації з метою уникнення негативного впливу у загальноприйнятому розуміння цього поняття.

Таким чином, основними, **базисними індикаторами** інформаційної безпеки з присутніми їм властивостями слід вважати наступні:

Базисний індикатор	**Властивість**
повнота інформації	віддзеркалення вичерпного характеру відповідності одержаних відомостей цілям збору; достатність для розуміння ситуації та прийняття рішення; характеристика, яка визначає кількість інформації необхідної та достатньої для прийняття вірного рішення
вчасність інформації	ознака того, що вона є саме тією, яка потрібна на даний момент; важливість, істотність у певний момент часу
вірогідність інформації	віддзеркалення дійсності (істинного стану справ); достовірність (міра наближеності інформації до першоджерела або точність передачі інформації);
конфіденційність інформації	властивість захищеності інформації від несанкціонованого доступу та спроб її розкриття користувачем, що не має відповідних повноважень
цілісність інформації	показник того, що дані повні, умови того, що дані не були змінені при виконанні будь-якої операції над ними, будь то передача, зберігання або представлення
доступність інформації	здатність забезпечення, при необхідності, своєчасного безперешкодного доступу до інформації, що цікавить
санкціонованість поширення інформації	процес надання інформації споживачам , в рамках обумовлених повноважень

На основі розгляду законодавчо окреслених на даний час шляхів запобігання реальним та потенційним загрозам у сфері інформаційної безпеки, які наводяться у законах України “Про основи національної безпеки” [6, ст. 8)], “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” [7, підрозділ 13 розділу ІІІ)] та Доктрині інформаційної безпеки України [2, розділ 4)], можна визначити

три основних шляхи, які на думку законодавців, забезпечать необхідний рівень національної інформаційної безпеки:

1. ***Створення, вдосконалення та розвиток нормативно-правових та організаційно-розпорядчих передумов*** практичної реалізації:

– конституційного права громадян на свободу слова, доступу до інформації;

– неможливості монополізації інформаційної сфери України;

– формування та реалізація державної політики національного духовного та культурного відродження, яка відповідає інтересам українського народу і визначає чіткі критерії і пріоритети формування інформаційної політики в соціальній сфері;

– прямої заборони неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– створення дієвої та прозорої системи громадського контролю за діяльністю органів державної влади і органів місцевого самоврядування;

– розвитку національної інформаційної інфраструктури та ресурсів із забезпеченням державної підтримки вітчизняного виробника інформаційної продукції та її конкурентоспроможності, в т.ч. й створення системи Суспільного телебачення і радіомовлення України;

– захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, здійснення правоохоронної діяльності в інформаційній сфері;

– гармонізації законодавства України з питань інформаційної безпеки з міжнародними нормами і стандартами;

– ефективної координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань.

2. ***Створення економічних передумов***, в першу чергу, на основі державної підтримки, для розвитку національної інформаційної інфраструктури та ресурсів із забезпеченням конкурентоспроможності вітчизняної інформаційної продукції та послуг, в т.ч. за рахунок впровадження новітніх технологій та наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну, спроможності протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави.

3. ***Забезпечення спроможності протидії інформаційно-психологічним операціям*** (створення повнофункціональної інформаційної інфраструктури держави із забезпеченням захисту її критичних елементів, в т.ч. розроблення та вдосконалення методів і засобів захисту інформації; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань)**.**

Узявши за основу наведені вище шляхи запобігання та усунення реальних та можливих загроз у інформаційній сфері, можна визначити, на макрорівні, наступні індикатори, які визначають рівень національної інформаційної безпеки та які, на думку автора, можна позначати як **реалізаційні індикатори**:

– Наявність та достатність нормативно-правової та організаційно-розпорядчої бази у сфері забезпечення інформаційної безпеки.

– Ефективність нормативно-правових та організаційно-розпорядчих передумов практичної реалізації запобігання та усунення наявних та можливих загроз у сфері інформаційної безпеки

– Достатність та ефективність економічної і програмно-технічної баз для запобігання та усунення реальних та можливих загроз у інформаційній сфері.

– Спроможність протидії інформаційно-психологічним операціям.

Цілком зрозуміло, що, як поняття “інформаційна безпека”, внаслідок своєї сутності, є багатоаспектним, багатогранним, то й наведені реалізаційні складові, які не є вичерпними, є також багатоаспектними, багатоскладовими. Ця багатоаспектність обов`язково виявиться під час здійснення виміру або оцінки цих індикаторів, що буде зроблено у результаті подальших досліджень.

Знання індикаторів будь-якого процесу, в нашому випадку – інформаційної безпеки, дуже важливе, насамперед, з точки зору визначення наріжних, базових, принципових моментів цього процесу, але значно важливіше знати кількісні або якісні характеристики цих індикаторів, як сукупності їх складових – індикативних показників.

Саме вірне визначення відповідних індикаторів, необхідний (оптимальний) рівень їх деталізації, з подальшим виміром, кількісного або якісного, кожного індикатора та їх сукупності, надає чітке уявлення стану даної складової визначеного процесу (у нашому випадку – інформаційної безпеки). Саме питання оптимізації індикаторів стану інформаційної безпеки, окреслення їх індикативних показників та шляхів їх виміру є предметом подальших досліджень.

Окремо необхідно відзначити таку властивість інформаційної безпеки, як негативні наслідки застосування інформаційних технологій.

Особливість ця полягає не в тому, що зараз все більше застосовуються інформаційно-комунікаційні сучасні технології, які постійно розвиваються та вдосконалюються, а в тому, що навіть при збереженні повноти, цілісності, вірогідності та, навіть, зовнішнього вигляду, конфіденційності, новітні прийоми та технології доведення інформації, можуть мати зворотній ефект. Саме технології та окремі прийоми технології донесення інформації до свідомості громадськості, суспільства та окремої людини є, на даний час, визначальними.

Необхідно також враховувати, що саме застосування сучасних інформаційних технологій “породило” такі поняття, як “комп’ютерна злочинність” та “комп’ютерний тероризм”.

Відмітимо, що, наприклад, такий злочин у сфері інформаційних технологій, як крадіжка номерів кредитних карток і інших банківських реквізитів (фішинг), потребує знання якраз повної, вірогідної та цілісної інформації. Саме тому злочинці у даній сфері намагаються отримати саме таку інформацію за будь-яку ціну.

Решта злочинів у даній сфері, такі як, наприклад, поширення шкідливих вірусів, злом паролів, поширення протиправної інформації (наклепу, матеріалів порнографічного характеру, матеріалів, збуджуючих міжнаціональну і міжрелігійну ворожнечу і тому подібне) спрямовані на порушення нормальної, стабільної роботи інформаційних систем або окремих їх складових з метою, в першу чергу, спотворення наведених вище властивостей інформації.

Те саме можна сказати про комп’ютерний тероризм. Метою комп’ютерного тероризму є навмисне нанесення шкоди або загроза нанесення шкоди комп'ютерам і комп'ютерним мережам для досягнення політичних, ідеологічних, релігійних або інших подібних цілей, бо природа тероризму спрямована на викликання страху, жаху. Тобто, знов таки маємо справу зі спотворенням наведених вище властивостей інформації.

Крім того, сучасні інформаційні технології надали більше можливостей здійснення маніпулювання суспільною свідомістю, використання персональних даних, поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності та багато чого іншого.

Але, з методологічної точки зору, всі ці негативні наслідки застосування інформаційних технологій, а точніше – індикатори цих наслідків, зводяться, знов-таки, до вище наведених **базисних індикаторів** інформаційної безпеки

Цей погляд автора базується на тому, що головним завданням інформаційної безпеки є забезпечення змістовності, першоджерельності інформації та збереження історії звернення до неї поряд із забезпеченням своєчасності, санкціонованості доступу до цієї інформації та методів і засобів її розповсюдження.

На глибоке переконання автора, ключ вирішення дуже багатьох питань інформаційної безпеки знаходиться саме у спроможності виміру, якісному або кількісного, таких її базисних індикаторів – властивостей інформації, як повнота, вчасність, вірогідність, цілісність.

Це надзвичайно складна, у всіх аспектах, задача, але її, тим не менш, треба вирішувати, бо це вже є об’єктивною вимогою часу.

Висновки.

1. Основою інформаційної безпеки є інформація, яка має властивість формування, розширення, корегування, спотворення та ін. свідомості людини, її світогляду.

2. Особливість інформаційної безпеки полягає у тому, що людина знаходиться у перманентному стані прийняття рішення [8], головний вплив на який здійснює інформація завдяки своїх основних властивостей – повноти, вчасності, вірогідності, цілісності та конфіденційності поряд із її доступністю.

3. За аналогією з тим, що *“безпека – стан захищеності, коли кому-, чому-небудь ніщо не загрожує”* [9], *мож*на говорити, що *інформаційна безпека – стан захищеності людини, суспільства, коли відсутній негативний, у загальноприйнятому (унормованому), на даний час, розумінні, вплив на людину, суспільство та негативних наслідків від застосування сучасних інформаційних технологій.*

4. Повної, не кажучи вже про абсолютну, інформаційної безпеки не може бути за визначенням внаслідок сутності інформації та методів і засобів її розповсюдження. Можна говорити лише про рівень інформаційної безпеки, його співвідношення з бажаним.

5. Рівень інформаційної безпеки визначається на основі сукупності кількісних та якісних характеристик визначених її індикаторів.

6. Базою для визначення індикаторів, що характеризують рівень інформаційної безпеки є, насамперед, властивості інформації – повнота, вчасність, вірогідність, конфіденційність та цілісність, а також доступність інформації та режим її розповсюдження, наслідки застосування інформаційних технологій.

Базисними індикаторами рівня інформаційної безпеки є:

- повнота інформації;
- вчасність інформації;
- вірогідність інформації;
- конфіденційність інформації;
- цілісність інформації;
- доступність інформації;
- санкціонованість розповсюдження інформації.

7. До принципово важливих **реалізаційних індикаторів** оцінки рівня інформаційної безпеки на макрорівні слід віднести:

– наявність та достатність нормативно-правової та організаційно-розпорядчої бази у сфері забезпечення інформаційної безпеки;

– ефективність нормативно-правових та організаційно-розпорядчих передумов практичної реалізації запобігання та усунення наявних та можливих загроз у сфері інформаційної безпеки;

– достатність та ефективність економічної і програмно-технічної баз для запобігання та усунення реальних та можливих загроз у інформаційній сфері;

– спроможність протидії інформаційно-психологічним операціям.

Перспективи щодо подальших досліджень. Подальші дослідження, об`єктивно, повинні бути спрямовані, по-перше, на деталізацію (розкриття) реалізаційних індикаторів оцінки рівня інформаційної безпеки. По-друге – означення індикативних показників як базисних, так й реалізаційних індикаторів оцінки рівня інформаційної безпеки. По-третє – методології визначення кількісних/якісних параметрів означених індикативних показників.

Використана література

1. Додонов А.Г. Компьютерные информационно-аналитические системы : толковый словарь / А.Г. Додонов, Д.В. Ландэ, В.Г. Путятин. – К. : НВП “Видавництво “Наукова думка” НАН України”. – 2011. – 384 с.

2. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.

3. Фурашев В. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки / В. Фурашев // Інформація і право. – № 1(4)/2012. – С. 46-55.

4. Фурашев В. Сутність та визначення понять “інформаційна безпека” і “безпека інформації” / В. Фурашев // Правова інформатика. – № 2(34)/2012. – С. 51-59.

5. Про Стратегію національної безпеки України : Указ Президента України від 12.02.07 р. № 105/2007 // Офіційний вісник України. – 2007. – № 11. – С. 7. – Ст. 389.

6. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

7. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України. – 2007 р. – № 12. – С. 511. – Ст. 102.

8. Фурашев В. Сутність та визначення поняття “рішення” / В. Фурашев // Правова інформатика. – № 1(37)/2013. – С. 49-55.

9. Вікіпедія – вільна енциклопедія. – Режим доступу : //www.uk.wikipedia.org/wiki/Безпека

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~