УДК 001.6+004

І.О. Громико

Харківський національний університет ім. В.Н. Каразіна, Харків

КЛАСИФІКАЦІЯ КОМУНІКАБЕЛЬНОСТІ НОСІЇВ ІНФОРМАЦІЇ

У статті наведено варіант класифікації «комунікабельності носіїв інформації», який побудований на основі системного аналізу великої кількості термінів і визначень для сфери комунікацій.

Ключові слова: *захист інформації, комунікабельність носіїв інформації.*

Вступ

Постановка проблеми. При вивченні рівнів захищеності об’єктів інформаційної діяльності виникають деякі складнощі, пов'язані з інтерпретацією термінів, наведених в Загальній парадигмі захисту інформації (далі, - Парадигма захисту) і Загальному законі захисту інформації (далі, - Закон захисту). Наприклад, як показано [1], в методичному плані при забезпеченні захищеності інформації в першу чергу необхідно здійснити аналіз можливих шляхів поширення інформації, розглядаючи дискретні елементи середовища впливу - носії інформації з урахуванням їх параметрів, що істотно впливають на процес комунікацій.

Це дозволить забезпечити мінімальні втрати (енергії, інформативності, часу і пр.) переміщення інформації носіями і при її «переході» від одного носія до іншого.

Носії інформації є основними елементами процесів створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації [2, 3].

Слід вказати на те, що комунікабельність носіїв інформації повинна забезпечуватися (підтримуватися) як у динамічному режимі, коли змінюються координати інформації, так і в статичному. Прагнення охопити режими для всіх видів інформаційної діяльності привело в 2012-му році до формулювання Загального (основного) закону захисту інформації. При цьому, в останньому, як і в Парадигмі захисту, зберігається основний упор на режимні адекватність і комунікабельність носіїв інформації.

Узагальнене визначення носія встановлено в Державному стандарті України, як «матеріального об'єкту, що містить інформацію, яка підлягає захисту від загроз: витоку, можливості блокування або порушення цілісності» [4].

При цьому, під інформацією розуміються «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі», або «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» ([2] - в редакції 1992р. та 2011р.).

Носіями інформації є матеріальні об'єкти в матеріальному або польовому вигляді, що використовуються для зберігання, перенесення (переміщення, доставки та ін.) інформації. Носії класифікуються на основні (джерело і одержувач) і проміжні (допоміжні).

У більш доступній до розуміння формі, - до носіїв інформації відносяться матеріальні об'єкти, що забезпечують запис, зберігання і передавання інформації у просторі і часі. Однак, при таких «технократичних» визначеннях на другий план відходить роль людини, що знаходиться в соціумі. Людина є першоджерелом створення і збереження інформації з метою її перенесення в просторово-часовому континуумі.

У зв'язку з цим, документ СБУ вчасно роз'яснив ситуацію, вказавши на те, що людина також є носієм інформації [5].

По відношенню до захищеності інформації, Парадигма захисту дає таке визначення: « Інформація вважається захищеною, якщо при її переміщенні дотримується режимна адекватність комунікабельних носіїв інформації». Відповідно, розширюючи область застосування Парадигми захисту до статичних режимів здійснення інформаційних взаємодій носіїв.

Закон захисту встановлює, що «Інформація вважається захищеною, якщо при здійсненні інформаційної діяльності в ланцюгах інформаційних взаємодій носіїв інформації дотримується режимна адекватність і комунікабельність» .

Застосування цих визначень на практиці вимагає детальної інтерпретації кожного з термінів та їх словосполучень . Це дозволяє усунути багатозначність і помилковість при забезпеченні інформаційної безпеки на об'єктах.

Огляд досліджень та публікацій. У формулюванні парадигми використані лави термінів, які вимагають уточнення. До них відносяться також і словосполучення.

Наприклад, словосполучення "режимна адекватність", що склалося з термінів "режим" і "адекватність".

Режим - це сукупність норм для досягнення якоїсь мети.

Наприклад, для захисту інформації [6]. Тут обов'язково, з урахуванням нової редакції Закону України «Про інформацію», відкривається зміст режиму доступу до інформації, як передбаченого правовими нормами порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації.

Адекватність - (від лат. adaequatus - прирівняний, рівний) це відповідність, точність.

Наступне поняття, використане в парадигмі - комунікабельність (від лат. communicabilis - сполучний, сполучуваний).

Комунікабельність означає сумісність (здатність до спільної роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку - аналогових і дискретних, у телебаченні - з різним числом рядків розкладання телевізійного кадру); здатність до спілкування, товариськість [6].

Режимна адекватність носіїв інформації - це відповідність режимів доступу носіїв інформації (джерела й одержувача) при їх взаємодії.

Приклад режимної неадекватності: ознайомлення зі змістом секретного документа без права на доступ до секретної інформації.

Приклад режимної адекватності: особиста розмова двох людей, які бажають передати і відповідно одержати інформацію з обмеженим доступом, що є власністю одного з них.

Комунікабельні носії інформації - це носії інформації, здатні до взаємодії.

Приклад некомунікабельності носіїв: через сенсор - органи зору (очі) людини не здатні сприйняти мовну (акустичну) інформацію.

Приклад комунікабельності носіїв: через сенсор - органи зору – очі - люди здатні сприйняти інформацію, зафіксовану чорнилом на паперовому носії зрозумілою для них мовою при наявності освітлення.

Проміжні носії інформації, так само, як і носій-джерело, і носій - одержувач, повинні відповідати вимогам режимної адекватності й комунікабельності.

Режимна адекватність комунікабельних носіїв інформації - це здатність носіїв інформації брати участь в інформаційному обміні при відповідності режимів доступу.

У загальному випадку під інформаційною загрозою розуміється потенційне порушення безпеки, або ступінь імовірності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію.

З багатьох способів класифікації загроз інформації найбільш загальним є їх класифікація за результатами можливого впливу на інформацію:

- загрози порушення конфіденційності;
- загрози порушення цілісності;
- загрози порушення доступності.

Загрози конфіденційності спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача, який не має санкції на такий вид інформаційної взаємодії.

Під інформаційною взаємодією двох і більше носіїв інформації розуміється процес створення, передачі, прийому, перетворення і/або знищення інформації, представленої в будь-якій матеріальній формі (польова, речова) і вигляді (символи, графіка, анімація і пр.).

При цьому можуть бути реалізовані: зворотній зв'язок між носіями, запитно-відповідальна форма з використанням паролів, вибір варіантів змісту інформації та режимів роботи з нею (й т. ін.) [7].

Інформація зберігає конфіденційність, якщо дотримується насамперед, режимна адекватність носіїв інформації.

Загрози цілісності інформації направлені на заборонену режимом доступу (порядком одержання, використання, поширення і збереження інформації) зміну або перекручування, інформації, які призводять до порушення її якості чи повне знищення. Цілісність інформації може бути порушена навмисно, а також у результаті дії факторів середовища впливу, в якому перебуває носій інформації.

Інформація зберігає цілісність, якщо дотримується установлена режимна адекватність щодо правил її модифікації (видалення).

Всякий суб'єкт, який впливає на носія-джерело інформації з метою модифікації інформації, можна розглядати як носія інформації, що містить у собі уявлення про необхідну модифікацію (видалення) інформації носія-джерела інформації. У процесі модифікації відбувається переміщення модифікуючої інформації.

Вплив об'єктів, процесів, навколишнього середовища й інших факторів, які часто відносять до розряду "випадкових" - це невідповідність носія-джерела інформації встановленому режиму доступу, що часто приводить до порушення комунікабельності. Такий вплив є порушенням режимної адекватності і, як наслідок, комунікабельності носіїв інформації.

Загрози доступності (відмова в обслуговуванні) спрямовані на навмисне чи ненавмисне порушення комунікабельності носіїв інформації при їх інформаційній взаємодії.

Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо

зберігається комунікабельність носіїв інформації при їх взаємодії.

Аналіз більш як сотні джерел інформації показав, такий термін, як комунікація та його похідні: комунікабельність, комунікативність (та ін.) використовується в біо- та техносистемах і потребує деякої систематизації.

Метою статті є систематизація словосполучення «комунікабельність носіїв інформації» та розкриття її фізичного змісту при взаємодії носіїв в процесі здійснення інформаційної діяльності.

Основна частина

Термін комунікабельність носіїв інформації охоплює три середовища (три сфери), які своїми факторами надають на вплив на інформаційні взаємодії носіїв інформації. Їх можна розділити на такі сфери:

– соціум,

– технічна

– логічна.

Відповідно, комунікабельність носіїв інформації можна розмежувати (класифікувати) на соціальну, технічну і логічну (рис. 1).

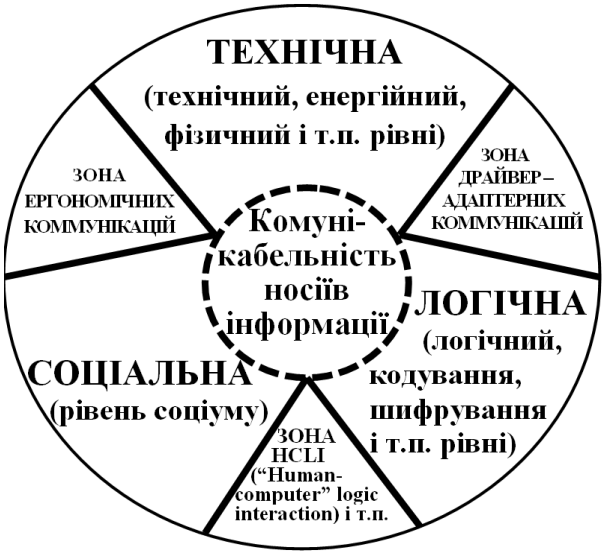

Рис. 1. Варіант класифікації комунікабельності носіїв інформації в сфері комунікацій.

Слід вказати, що в літературних джерелах ці поняття суттєво «перемішані».

Наприклад, у сфері соціуму деякими авторами виділяється поняття (А) «технічна комунікація» на рівні професіонала - менеджера, що володіє техніками типу NLP соціального «приєднання» до співрозмовника.

Також, в інших джерелах, (Б) «технічна комунікація» трактується, як набір методів, якими практикуючі фахівці користуються, щоб визначити технічні процеси викладені у документі чи застосовані для виготовлення продукції.

Крім цього, у визначенні (В) «технічної комунікації», закладена головна практична мета - створити легко доступну інформацію для специфічної аудиторії. Наведемо деякі пояснення до рис. 1.

1. Соціальна комунікабельність носіїв інформації.

Уявлення про інформаційну сфері соціуму розглядалися ще з часів античності (Платон, Протагор) і порушували цю сферу, як елемент соціального управління (Аристотель, Цицерон).

Розвиток інформаційних технологій призвів до того, що дев'ять десятих усієї інформації сьогодні циркулює в технічній радіоелектронній формі, що привертає до цієї проблеми фахівців у галузі технічних наук, які займаються ергономічними питаннями комп'ютерної інформації. Але, справа в тому, що сам процес передачі інформації є соціальним за своєю суттю, в силу того, що в кінцевому рахунку він полягає в передачі інформації (змісту свідомості) від однієї людини до іншої. Людина є як виробником, так і споживачем інформації. Соціальні комунікації це передача інформації, як особлива форма інформаційних відносин між людьми. У зв'язку з цим, зміст і сенс інформаційної сфери соціуму необхідно розглядати в широкому соціально - технологічному контексті [8].

2. Технічна комунікабельність носіїв інформації.

Техносфера — сфера, яка містить штучні технічні споруди, які виготовляються та використовуються людиною. Комунікації між ними та їх якість є характеристикою технічної комунікабельності носіїв інформації.

«Світ речей, сукупність технічних засобів і пристроїв, продуктів діяльності людини – світ, створений людиною [9].

3. Логічна комунікабельність носіїв інформації.

Під логічною комунікабельністю носіїв інформації розуміється область прикладної логіки інформаційно-комунікаційних пристроїв і систем, як сфери застосування науки логіки; різноманітність практичного використання математико-логічних теорій, унаслідок чого логіка виконує методологічну функцію і набуває прикладного значення та відноситься до комп'ютерної логіці, як базису IT (інформаційних технологій) [10].

На рис. 1 виділені граничні зони, які є окремими самостійними науковими напрямками. З них, в першу чергу, найбільш вивчена зона ергономічних комунікацій. Потім, по зменшенню вивченості, слідує зона технічних комунікацій і HCLI – сучасна зона програмно-соціальних комп'ютерних комунікацій.

Ці граничні зони, вимагають додаткового докладного опису, що виходить за обсягом і спрямованістю цілей за рамки цієї статті.

Висновки

1. Комунікабельність носіїв інформації узагальнено охоплює три сфери комунікацій: соціальну, технічну (техносферу) і логічну. У них комунікації якісно відрізняються.

2. На кордонах дотику сфер утворені граничні зони, що представляють собою окремі наукові напрямки для додаткових досліджень, спрямованих на підвищення якісних і кількісних параметрів (швидкість, підвищення обсягу переданої інформації (трафік), зменшення спотворень інформації, зниження числа помилок і пр.) комунікацій.

Список літератури

1. Громыко И.А. Дискретизация среды распространения информации / И.А. Громыко // Системи обробки інформації. Збірник наукових праць. Видавництво Харківського університету Повітряних Сил ім.. І. Кожедуба, – Х.: ХУПС, 2013. – Вип. 2 (109). – С. 178-182.

2. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. - №48. – С. 650.

3. Громико І.О. Загальна парадигма захисту інформації / І.О. Громико // Науково-практичний посібник «Інформація та інформатизація». 2-е видання, доп. й перероб. – Харків: Вид-во. НУВС, 2003 р. - 724 с.

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

5. НД ТЗИ 1.1-002-99 Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ ДСТЗІ СБ України. – К., 1999.

6. Советский энциклопедический словарь / Научно-редакционный совет: А. М. Прохоров (пред.). - М.: "Советская Энциклопедия", 1981. - 1600 с.

7. Громыко И.А. Общий закон защиты информации / И.А. Громыко // Вестник Харьковского национального университета имени В.Н. Каразина. Серия: «Математическое моделирование. Информационные технологии. Автоматизированные системы управления». – № 1037, вып. 20. – 2012. – С. 43-56.

8. Кибанов В.А. Информационная сфера социума. Роль и место в системе социального управления. : Диссертация на соискание уч. степени канд. социол. наук: 22.00.08 : Москва, 2004 154 с. РГБ ОД, 61:04-22/101-8.

9. Словники ABBYY Lingvo (Uk-Uk) техносфера Explanatory (Uk-Uk). Електронний ресурс. Режим доступу: http://www.lingvo.ua/uk/Interpret/uk-uk/Техносфера.

10. Карамишева Н.В. Логіка (теоретична і прикладна) : навч. посіб. / Н. В. Карамишева. – К. : Знання, 2011. – 455 с.ISBN: 978-966-346-725-2.

Надійшла до редколегії 5.08.2013

Рецензент: д-р техн. наук, проф. С.Г. Рассомахін, Харківський національний університет ім. В.Н. Каразіна, Харків.

КЛАССИФИКАЦИЯ КОММУНИКАБЕЛЬНОСТИ НОСИТЕЛЕЙ ИНФОРМАЦИИ

И.А. Громыко

В статье приведён вариант классификации «коммуникабельности носителей информации», который получен на основе системного анализа большого числа терминов и определений для сферы коммуникаций.

Ключевые слова: *защита информации, коммуникабельность носителей информации.*

CLASSIFICATION OF SKILL TO COMMUNICATE OF DATA CARRIERS

I.O. Gromyko

In this article the option of classification of skill to communicate of the information carrier is shown. Option is obtained through a systematic analysis of a large number of terms and definitions for the sphere of communications.

Keywords: *information security, skill to communicate of data carriers.*