DOI https://doi.org/10.30525/978-9934-26-686-7-4

ГОЛОВНИЙ ЗАКОН ЗАХИСТУ ІНФОРМАЦІЇ

Громико І. О.

ВСТУП

Сучасна ситуація в галузі захисту інформації така, що спроби спиратися на деякі суттєві терміни, що використовуються в законах, постановах, підручниках та навчальних посібниках із захисту інформації іноді призводять до розмитості розуміння реальних процесів інформаційної діяльності. В результаті, упускаються з першого погляду «дрібні» нюанси інформаційної термінології, які надалі породжують непорозуміння серед адміністраторів та операторів ЕОМ, володарів та користувачів інформацією, що виконують свої обов'язки, знаходячись у різноманітних ланцюгах інформаційної взаємодії.

Як мінімум, такий стан розвитку інформаційних технологій створив тупикові ситуації для людей що познають основи інформаційної безпеки – працівників служб служби безпеки, студентів, та ін. Взагалі, це гальмує процес вивчення і розвитку широкого тематичного спектру діяльності носіїв інформації сучасного інформаційного простору[1].

Стан такої ситуації протягом великого тимчасового періоду (десятки років…!) переконав автора в необхідності проведення нового етапу досліджень, у ході яких було виявлено декілька суттєвих "прогалин" у інформаційної теорії взаємодії носіїв інформації. Особливо це мало відношення до забезпечення безпеки інформації в умовах різноманітних загроз. Частина цих загроз була породжена відмінностями режимів комунікабельності носіїв інформації. Саме ці питання на цей момент залишаються невивченими або невирішеними при здійсненні інформаційної діяльності.

Метою дослідження є формулювання головного закону захисту інформації на підставі аналізу інформаційної діяльності носіїв інформації в умовах впливу інформаційних загроз.

Унікальність отриманих результатів підтверджена патентами України[2,3,4,5]. Вже зараз 20.02. 2026 року в допомогу збройним силам розроблені основи реалізації способу та застосуванню приладу принципово нової військової техніки і подані заявки на отримання патентів України.

---

[1] Громико І.О. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання : монографія. Харків : ХНУ ім. В.Н.Каразіна, 2014. 216 с

[2] Спосіб знешкодження вибухового пристрою : пат. Україна : МКП F42D 5/04. № 7238 ; заявл. 11.08.2006 ; опубл. : 15.06.2005, Бюл. № 5

[3] Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. № 32620 ; заявл. 26.05.2008 ; опубл. : 26.05.2008, Бюл. № 10

[4] Там само.

[5] Там само. № 114388 ; заявл. 11.08.2006 ; опубл. : 10.03.2017, Бюл. № 5.

Велика кількість доповідей на міжнародних та вітчизняних конференціях, секцій що присвячені захисту інформації.

Автор мінімізував кількість застосованих інформаційних джерел, яких в оригіналі роботи більш 80-ти, та прикладів практичного застосування досліджень, в тому числі – рекомендацій та патентів як для захисту інформації в службових кабінетах, так й для застосування в діючих підрозділах збройних сил України.

Дослідження проводилися на території кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту ХНУ ім. В.Н.Каразіна, інших факультетів та кафедр, та у дружніх наукових центрах Харкова. Особливу подяку автор висловлює колективу «Харківського регіонального науково-виробничого центру стандартизації, метрології та сертифікації», що дозволило суттєво підвищити якість науково-практичних досліджень автора у галузі інформаційної радіофізики.

В результаті багаторічних досліджень, включаючи експерименти, автором сформульований «Загальний закон захисту інформації»:

«Інформація вважається захищеною, якщо під час здійснення інформаційної діяльності обов'язково і одночасно виконуються дві головні вимоги до інформаційних ланцюгів взаємодії носіїв інформації:

1) «режимна адекватність» носіїв інформації;

2) «режимна комунікабельність» носіїв інформації» (UA).

"Information is considered protected if, during the implementation of information activities, two Key (Primary, Core and Basic) requirements for information chains of interaction of information carriers are necessarily and simultaneously fulfilled:

1) "regime adequacy" of information carriers;

2) "regime communicability" of information carriers." (ENG).

1. Інформаційна діяльність носіїв інформації

При проведенні науково-дослідницьких робіт автор використовував керівні та науково-інформаційні державні довідники, документи та рекомендації сайтів штучного інтелекту. Тому посилання на джерела в даному випадку не приведені.

1.1. Деякі визначення та термінологія

Інформація – це зафіксоване носієм, та на носії, уявлення про предмети, процеси, події, природні явища (тощо) як відображення реального світу.

Інформація завжди знаходиться з носієм та завжди має свою цінність, бо нейтральної інформації не існує.

Відомості – це будь-які дані, повідомлення, факти або інформація про осіб, події, явища, процеси чи предмети, які можуть бути зафіксовані носіями або на матеріальних носіях.

Дані (data) – це формалізоване подання фактів, чисел, понять або інструкцій, зафіксоване на носії (або в пам'яті комп'ютера), яке придатне для оброблення, передавання або інтерпретації людиною чи автоматичними системами. У комп'ютерних науках (IT): дані – це формалізоване подання

інформації, придатне для інтерпретування, пересилання чи оброблення за допомогою автоматичних засобів або людини (згідно зі стандартом ISO/IEC 2382:2015).

Об'єкт захисту – це об'єкт, який підлягає захисту від негативних дій «джерела загроз». Джерело загроз умисно або випадково здійснює чи планує напад/вплив на об'єкт захисту. В нашому ракурсі досліджень ми під «об'єктом захисту» розуміємо інформацію, інформаційні та інші процеси що застосовують при здійсненні інформаційної діяльності (або здійснюються згідно завданих програм) у ланцюгах інформаційної взаємодії носіїв інформації, які необхідно захищати відповідно до мети цифрової безпеки

Захист – це дія за значенням не допустити впливу на «об'єкт захисту» загрозам, які мають на меті запобігти порушенням прав будь-кого.

Метою захисту інформації є унеможливлення або суттєве утруднення реалізації загроз для інформації, що є власністю держави, сприяння реалізації законних інтересів та прав фізичних і юридичних осіб, державних органів здійсненню ними своїх завдань і функцій, а також загроз, реалізація яких може нанести державі, суспільству або особі політичні, економічні, моральні та інші збитки. Метою захисту інформації є забезпечення її конфіденційності, цілісності та доступності (тріада CIA: Confidentiality, Integrity, Availability). Це комплекс заходів для запобігання несанкціонованому доступу, викраденню, знищенню, модифікації або витоку даних, що мінімізує ризики та збитки для користувачів, компаній або держави.

Поняття: «володілець», «володар», «власник», або «загрози інформації», «загрози для інформації», «інформаційні загрози» та «кіберзагрози» повинні розглядатися з повним надаванням змісту та суворим відстежуванням інформаційних **причинно-наслідкових зв'язків** між авторами, власниками, володільцями, володарями та користувачами щодо наслідків інформаційної діяльності в ланцюжках взаємодії носіїв.

Загроза (англ. threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Кібератака (англ. cyber-attack) – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

1.2. Режимна адекватність носіїв інформації

На протязі багатьох років та на конкретних прикладах практика доводить, що постійно у ланцюгах інформаційної взаємодії носіїв інформації «чогось не вистачає», якихсь елементів чи додаткових дій у системах захисту інформації. У всіх державах світу фахівцями систем захисту інформації повністю не враховані деякі динамічні зовнішні чи внутрішні чинники, яким спочатку не надають істотного значення і які в реальних ситуаціях починають превалювати за значимістю над застосованими сучасними методами та засобами захисту інформації.

Внаслідок цього – загрози щодо інформації «успішно» реалізуються конкурентами, розвідувальними службами іноземних держав, терористами та ін.

Попередньо назвемо ці чинники. До таких належать:

- режимна адекватність носіїв інформації;
- комунікабельність носіїв інформації.

Режим, це передбачений правовими нормами доступ/взаємодія носіїв до інформації в процесі: створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації[6].

Адекватність – від лат. adaequatus – прирівняний, рівний.

Режимна адекватність носіїв інформації – це відповідність режимів допуску всіх носіїв інформації за їх взаємодії. Під взаємодією слід розуміти здійснення носіями будь-яких видів інформаційної діяльності.

Режим захисту інформації це система заходів, правил, запроваджуваних для досягнення мети захисту інформації.

Звернемо увагу на класифікацію інформації згідно доступу. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Таємна інформація, або «державна таємниця» – вид інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєве важливим інтересам України і які визнані у порядку, встановленому законом, державною таємницею та підлягають охороні з боку держави[7,8].

---

[6] Про інформацію : Закон України від 2 жовтня 1992 р. № 48 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.03.2026)

[7] Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII / Верховна Рада України. URL : https ://zakon.rada.gov.ua/laws/show/ 3855-12#Text; Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

[8] Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

Службова інформація може міститися лише в документах суб'єктів владних повноважень, визначених у статті 13 Закону України «Про доступ до публічної інформації», що стосується їх діяльності. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування» (ДСК). На документах, що містять службову інформацію з:

- мобілізаційних питань, додатково проставляється відмітка "Літер "М";
- питань криптографічного захисту службової інформації, – відмітка "Літер "К";
- питань спеціальної інформації, – відмітка "СІ".

Категорії документів, на яких проставляється відмітка "Літер "К", визначаються нормативно-правовими актами Адміністрації Держспецзв'язку.

Забороняється використовувати для передачі службової інформації відкриті канали зв'язку.

Закон України «Про доступ до публічної інформації», зокрема стаття 9, окреслює коло інформації, яка може належати до категорії «службова»:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Отже, якщо інформація належить до вказаного кола, вона може отримати статус «службової».

Належати до службової така інформація може відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації», тобто після застосування так званого «трискладового тесту». Так, обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Доступ до службової інформації обмежується лише за умови наявності всіх трьох вимог. При відсутності хоча б однієї з них інформація є відкритою (частина 2 статті 6 Закону України «Про доступ до публічної інформації»).

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

2. Комунікабельність як об'єднуючий універсальний термін

Збирання інформації є інформаційним аналогом її отримання особисто чи/та за допомогою технічних систем, яким відведено одну з провідних ролей у будь-яких видах інформаційної діяльності. Найбільш ємне і майже безпомилково цей інформаційний процес здійснює комп'ютерна система з елементами штучного інтелекту (***ШІ***).

Процес збору інформації супроводжується пошуком, оцінюванням, смисловим фільтруванням, приведенням у форму, зручну для подальшого використання, та іншими діями, які неможливі без здійснення **комунікацій** – початкового процесу обміну інформацією між носіями.

Повсякденне тлумачення терміну «**комунікації**» легко простежити у довідковій літературі.

У тлумачному словнику В. І. Даля (1881) слово «комунікація» тлумачилося як «шляхи, дороги, засоби зв'язку місць». Саме у цьому сенсі уродженець Полтавської області М. В. Гоголь писав: «Невський проспект є загальна комунікація Петербургу». Комунікація (від лат. communicatio – єдність, передача, з'єднання, повідомлення, пов'язане з дієсловом лат. communico – роблю спільним, повідомляю, з'єдную, похідним від лат. communis – спільний) – це процес обміну інформацією (фактами, ідеями, поглядами, емоціями тощо) між особами та системами з елементами штучного інтелекту (ШІ), спілкування за допомогою вербальних і невербальних засобів із метою передавання та одержання інформації.

Різноманітні види й способи комунікації можна поділити на три групи: усну, письмову й візуальну.

Далі ми розглянемо парадігмальне тлумачення терміну «комунікація».

Термін «комунікація» використовується багатьма суспільними, біологічними, технічними науками, і найчастіше мають на увазі елементарну схему комунікації (Рис. 1).

Рис. 1. Елементарна схема комунікації

Елементарна схема показує, що комунікація передбачає наявність щонайменше трьох учасників: носій – передавальний об'єкт (комунікант), носій (з повідомленням), носій – приймаючий об'єкт (реципієнт).

На відміну від елементарної парадігмальна схема (Рис. 2) передбачає наявність носіїв інформації, які комунікабельні настільки, що при переміщенні інформації з одного носія на інший загрози інформації не реалізуються і вона зберігає свої властивості: конфіденційність, цілісність та доступність.

Рис. 2. Парадігмальна схема комунікацій

В обох схемах ми спрощено не показує мо джерела завад (шуму та ін.).

Комунікація – це різновид інформаційної взаємодії між носіями. Для відмежування комунікації з інших інформаційних процесів покажемо її відмітні ознаки. Учасниками комунікації можуть бути:

- представники соціуму – окрема людина або група людей аж до суспільства в цілому (а також тварини – зоокомунікація);
- елементи техносфери – «технічні засоби прийому, передачі, обробки, зберігання і т. д. інформації» (далі, – ТЗПІ), а також «допоміжні технічні засоби та системи» (далі, – ДТЗС);
- програмні інформаційні продукти як об’єкти інтелектуальної діяльності, що використовуються спільно з ТЗПІ та ДТЗС.

Хтось з носіїв є джерелом, хтось – одержувачем інформації або обмін інформацією є «взаємним».

Комунікації властива доцільність чи функціональність.

Доцільність може виявлятися у кількох формах:

- переміщення носія з інформацією у геометричному просторі «з пункту А до пункту В» – у цьому полягає мета транспортної чи енергетичної комунікації;
- мета взаємодіючих носіїв полягає не тільки в обміні матеріальними предметами (конверти з листами, магнітні диски або електронні флеш-носії), а й у повідомленні один одному сенсів («смислів»), що мають особливу (смислову) природу (якісна чи смислова характеристика інформації). Носіями смислів є знаки, символи, тексти, що мають зовнішню, чуттєво сприймається форму і внутрішній умоглядний зміст. Можна дати ще одне загальне тлумачення: комунікація є опосередкована та доцільна взаємодія у просторі та в часі.

Залежно від знаходження носіїв у просторово-часовому континуумі слідує типізація комунікації, представлена на Рис. 3.

Як правило, процес переміщення інформації супроводжується узгодженням, яке включає процес приведення зібраної інформації до стандартів, розроблених для даного класу систем. Інакше без стандартизації позитивний результат процесу одержання (збору) інформації стає проблематичним.

Комунікація		
Технічна	**Соціальна**	**Логічна**
технічний, енергетичний, фізичний і т. п. типи.	смисловий, чуттєвий, психічний, технічний, енергетичний, фізичний і т.п. типи.	кодування, шифрування, кількісний, якісний і т. п. типи.

Рис. 3. Типізація комунікації

У плані інформаційної безпеки стандартизація як вид інформаційної діяльності має кінцеву мету встановлення для носіїв інформації норм, правил, характеристик та ін., які знижують ймовірність реалізації загроз для інформації шляхом забезпечення соціальної, технічної та логічної (семантичної, мовної) сумісності носіїв інформації.

Закон України показує цей процес у більш узагальненому вигляді: «Стандартизація – діяльність, що полягає в установленні положень для загального та неодноразового використання щодо наявних чи потенційних завдань і спрямована на досягнення оптимального ступеня впорядкованості у тому числі й задач інформаційної безпеки»[9].

В останні кілька років багато хто почав говорити про сумісність як інтероперабельність. Питання навіть виносилося на обговорення у міжнародних організаціях та на політичній арені. Як результат, отримано більш чітке визначення термінів в дослідженні IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens)[10].

«Інтероперабельність – це здатність інформаційних та комунікаційних технологій та бізнес-процесів, які ними підтримуються, до обміну даними та забезпечення обміну інформацією та знаннями».

1. Організаційна сумісність (соціальна, – авт.).

Сюди належить визначення бізнес-цілей, моделювання бізнес-процесів та забезпечення співпраці установ, які бажають обмінюватися інформацією (можуть мати відмінності у внутрішніх структурах та процесах).

2. Семантична сумісність (логічна, мовна).

Забезпечує зрозумілість процесу обміну інформацією для інших програм, які спочатку не були розроблені для цієї мети. Семантична сумісність дозволяє

[9] Про стандартизацію. Закон України від 5 червня 2014 року № 1315-VII Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/1315-18#Text

[10] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004]. https://www.ab.gov.tr/files/tarama/tarama_files/10/SC10EXP_ IDABC.pdf

об’єднати отриману інформацію з іншими інформаційними ресурсами для подальшої обробки. Як приклад семантичної сумісності браузерів показано Таблицю 1, яка не потребує додаткових пояснень сумісності[11].

Таблиця 1

Підтримка браузерами семантичних елементів

Браузер	IE	Firefox	Chrome	Safari	Opera	Safari iOS	Android
Мінімальна підтримувана версія	9	4	8	5	11.1	4	2.1

3. Технічна сумісність

Сюди входять технічні аспекти сумісності комп’ютерних систем та сервісів, такі як: відкриті інтерфейси, сервіси обміну інформацією, інтеграція даних та програмного забезпечення, подання даних, доступність та служби безпеки.

Таким чином, – комунікабельність (від пізньолат. communicabilis – сполучний, сполучений): 1) сумісність (здатність до спільної роботи (взаємодії – Авт.)) різнотипних систем передачі; 2) здатність до спілкування, товариськість.

Якщо порівняти смислове значення термінів «інтероперабельність» та «комунікабельність», то стає видно смислову ширину другого терміну, який охоплює всі три сторони терміну «сумісність». Одночасно комунікабельність узагальнено охоплює значення терміну «узгодженість» з такими його синонімами, як: узгодженість, злагодженість, струнікість; сумісність, несуперечність, контактність та ін.

Частота застосування терміну «комунікабельність» становить приблизно 30 відсотків у загальній лексиці, психології та автоматиці третину від загальної кількості застосувань. Тільки у медицині вона складає 8 відсотків від всіх термінів.

З огляду на те, що людина є носієм інформації, часто застосовують термін «сприйняття» інформації, що охоплює технічну сферу та сферу соціуму.

Сприйняття – процес перетворення відомостей у технічну систему чи живий організм із зовнішнього світу, у форму, придатну до подальшого використання. Розрізняють статичне та динамічне сприйняття

Сучасні інформаційні системи створюються, зазвичай, з урахуванням комп’ютерів і через складності мають розвинену систему сприйняття. Штучно – інтелектуальне (ШІ) сприйняття інформації представляє досить складний комплекс програмних та технічних засобів. Для розвинених систем сприйняття можна виділити кілька етапів переробки інформації, що надходить: попередня обробка для приведення вхідних даних до стандартного для даної системи виду, виділення в інформації вступників семантично і прагматично значущих інформаційних одиниць, розпізнавання об’єктів і ситуацій, корекція

[11] Браузерна сумісність семантичних елементів. [Електронний ресурс]. URL : http://professorweb.ru/my/html/html5/ level1/1_7.php

внутрішньої моделі світу (та ін.) від датчиків (сенсорів, аналізаторів), що входять до комплексу технічних засобів системи сприйняття, організується сприйняття зорового, акустичного та інших видів інформації.

Таким чином, можна стверджувати, що у певних випадках синонімами терміну «комунікабельність» є: узгодженість, сумісність, злагодженість, інтероперабельність, комунікативність та багато інших, що належать до сфер соціальних, технічних та/або логічних контактів. Застосування терміну «комунікабельність» найбільш ємне охоплює сфери сумісності інформаційних взаємодій носіїв інформації.

3. Класифікація «комунікабельності носіїв інформації»

Зрозуміло, що:

- комунікабельні носії інформації – це носії інформації які здатні до безпомилкової взаємодії:
- комунікабельність носіїв інформації – це здатність носіїв інформації брати безпомилкову участь у інформаційних процесах;
- режимна комунікабельність носіїв інформації – це здатність носіїв інформації брати безпомилкову участь (тобто з унеможливленням реалізації загроз інформації) у інформаційних процесах.

Існують і проміжні носії між носієм-джерелом і носієм-отримувачем інформації. Вони, та й весь їх інформаційний ланцюжок, так само, як і «носій-джерело та носій-отримувач», повинні відповідати вимогам комунікабельності.

Порушення комунікабельності перериває дозволені (санкціоновані) режимом доступу процеси переміщення інформації. Інформація зберігає конфіденційність, цілісність та доступність, якщо зберігається комунікабельність всього інформаційного ланцюга носіїв інформації за їх взаємодії між джерелом та отримувачем.

Аналіз понад сотні джерел інформації показав, що «комунікабельність носіїв інформації» потребує деякої систематизації та розкриття її фізичного змісту при взаємодії носіїв у процесі здійснення інформаційної діяльності.

Як було розглянуто раніше, комунікабельність носіїв інформації охоплює три середовища (сфери): соціальне, технічне та логічне. Вони своїми факторами впливають на процеси інформаційних взаємодій носіїв інформації (Рис. 5). Їх можна виділити (класифікувати) як три основні класи, що об’єднуються трьома прикордонними підкласами (зонами), які будуть наведені далі.

З середовищ впливу на комунікабельність носіїв інформації можна виділити (класифікувати) три основні класи, що об’єднуються трьома прикордонними зонами.

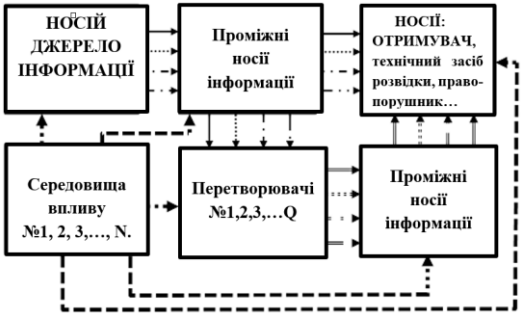

Рис. 5. Узагальнена структурна схема комунікації носіїв інформації на прикладі каналу витоку інформації

Слід зазначити, що у літературних джерелах ці поняття суттєво «перемішані». Наприклад, у сфері соціуму деякими авторами виділяється поняття «технічна комунікація» (а) на рівні професіонала – менеджера, який володіє техніками соціального «приєднання» до співрозмовника, наприклад, NLP. Також в інших джерелах «технічна комунікація» (б) трактується як набір методів, якими практикуючі фахівці користуються, щоб визначити застосовність технічних процесів, викладених у документі для виготовлення певного виду продукції. Крім цього, у визначенні «технічної комунікації» (в) закладено головну практичну мету – створити легкодоступну інформацію для аудиторії.

Класифікація та зони розмежування комунікабельностей носіїв інформації наведено на Рисунку 6.

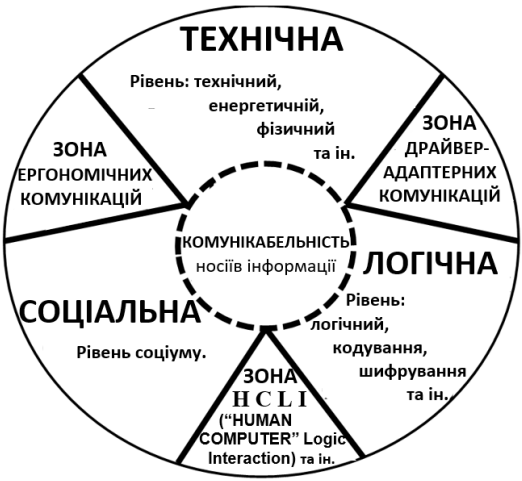

Рис. 6. Класифікація комунікабельності носіїв

А. **Соціальна комунікабельність** носіїв інформації

Подання про інформаційну сферу соціуму розглядалося ще з часів античності (Платон, Протагор), які представляли цю сферу як елемент соціального управління (Арістотель, Цицерон). Стрімкий розвиток інформаційних технологій призвів до того, що дев'ять десятих усієї інформації сьогодні циркулює в технічній «радіоелектронно- цифровій» формі та залучає до забезпечення соціальної комунікабельності фахівців у галузі технічних наук, які займаються вирішенням ергономічних питань у галузі комп'ютерної інформації.

Справа в тому, що сам процес передачі інформації по суті є соціальним через те, що в кінцевому рахунку він полягає в передачі інформації («синонімів»: змісту, відомостей, даних і т.п.) від однієї людини до іншої.

Людина (носій інформації…) є як виробником – джерелом, так і споживачем – одержувачем інформації. Тому соціальні комунікації є інформаційним процесом поширення інформації як особливої форми інформаційних відносин між людьми. У зв'язку з цим сенс та зміст інформаційної сфери соціуму необхідно розглядати у широкому соціально-технологічному контексті.

Б. **Технічна комунікабельність** носіїв інформації

Техносфера – це сфера, що містить штучні технічні споруди та пристрої, що виготовляються та використовуються людиною. Комунікації між ними та їх якість є характеристикою технічної комунікабельності носіїв інформації[12].

В. **Логічна комунікабельність** носіїв інформації

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

Будь-яке порушення комунікабельності носіїв інформації істотно збільшує вірогідність реалізації негативного впливу загроз на інформацію.

ВИСНОВКИ

Підсумовуючи результати багаторічних спостережень, публікацій, зауважень, відгуків та корекцій можна зробити позитивний висновок про те, що головний закон захисту інформації дає досить точну відповідь на запитання: «У яких випадках можна вважати інформацію захищеною»[13,14,15].

---

[12] Словники ABBYY Lingvo (Uk-Uk) техносфера Explanatory (Uk-Uk) [Електронний ресурс]. URL : http://www.lingvo.ua/uk/Interpret/uk-uk/Техносфера

[13] Громико І.О. Головний закон захисту інформації. Частина друга. Collection of scientific papers «Scientia». Section 9. Information technologies and systems. DOI 10.36074/scientia-16.08.2024 – Singapore, Republic of Singapore.- August 16, 2024. p. 45-50

[14] Громико І.О. Головний закон захисту інформації. VII Міжнародна науково-практична конференція "Theoretical and empirical scientific research: concept and trends"- Section XI Information technologies and systems – DOI 10.36074/logos-16.08.2024.001 – м. Оксфорд, Сполучене Королівство. 16 серпня 2024 р. 177-188

«Інформація вважається захищеною, якщо під час здійснення інформаційної діяльності обов'язково і одночасно виконуються дві головні вимоги до інформаційних ланцюгів взаємодії носіїв інформації:

1) «режимна адекватність» носіїв інформації;

2) «режимна комунікабельність» носіїв інформації» . (UA)

"Information is considered protected if, during the implementation of information activities, two Key (Primary, Core and Basic) requirements for information chains of interaction of information carriers are necessarily and simultaneously fulfilled:

1) "regime adequacy" of information carriers;

2) "regime communicability" of information carriers." (ENG).

АНОТАЦІЯ

Базуючись змістом Законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та «Про основні засади забезпечення кібербезпеки України» та державними стандартами і нормативними документами автор спробував знайти відповідь на запитання: «Коли інформацію можна вважати захищеною?». При чому відповідь повинна була містити і статичний, і динамічний стани носіїв інформації які приймають участь в інформаційній діяльності. Перша частина «Головного закону захисту інформації» була розроблена майже 10 років тому і мала назву «Загальна парадигма захисту інформації». І тільки у теперішній час вдалося повністю дослідити реальні інформаційні сучасні процеси що дозволило сформулювати визначення «Головного закону захисту інформації» в тому вигляді, який надається в даній науковій статті. Результати опубліковані у наукових збірниках декількох Міжнародних конференцій. Зауважень, поправок та корекцій на наступний момент до автора не надійшло. На думку автора, – Головний закон захисту інформації має право на життя.

Література

1. Громико І.О. Загальна парадигма захисту інформації: проблеми захисту інформації в аспектах математичного моделювання : монографія. Харків : ХНУ ім. В.Н.Каразіна, 2014. 216 с.

2. Спосіб знешкодження вибухового пристрою : пат. Україна : МКП F42D 5/04. №7238 ; заявл. 11.08.2006 ; опубл. : 15.06.2005, Бюл. № 5.

3. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №32620 ; заявл. 26.05.2008 ; опубл. : 26.05.2008, Бюл. № 10.

4. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №107207 ; заявл. 27.11.2015 ; опубл. : 25.05.2016, Бюл. № 10.

---

[15] Громико І.О. Пірамідальна модель доступу громадянина до державної таємниці. Збірник доповідей VI міжнародної науково-практичної конференції "Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи" 29 жовтня 2025 р./ Міністерство оборони України, НУОУ. УДК: 355.451. К.: НУОУ, 2025. 237 с. Ст. 131-135.

5. Спосіб визначення внутрішніх дефектів у стінах приміщень : пат. Україна : МКП G01B 11/16. №114388 ; заявл. 11.08.2006 ; опубл. : 10.03.2017, Бюл. № 5.

6. Про інформацію : Закон України від 2 жовтня 1992 р. № 48 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.03.2026).

7. Про державну таємницю : Закон України від 21 січня 1994 р. №3855-XII / Верховна Рада України. URL : https ://zakon.rada.gov.ua/laws/show/ 3855-12#Text

8. Наказ служби безпеки України № 383 від 23.12.2020р. (Редакція станом на 09.09.2024)

9. Про стандартизацію. Закон України від 5 червня 2014 року № 1315-VII Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/1315-18#Text

10. Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004]. https://www.ab.gov.tr/files/tarama/tarama_files/10/SC10EXP_ IDABC.pdf .

11. Браузерна сумісність семантичних елементів. [Електронний ресурс]. URL : http://professorweb.ru/my/html/html5/ level1/1_7.php

12. Словники ABBYY Lingvo (Uk-Uk) техносфера Explanatory (Uk-Uk) [Електронний ресурс]. URL : http://www.lingvo.ua/uk/Interpret/uk-uk/Техносфера

13. Громико І.О. Головний закон захисту інформації. Частина друга. Collection of scientific papers «Scientia». Section 9. Information technologies and systems. DOI 10.36074/scientia-16.08.2024 – Singapore, Republic of Singapore.- August 16, 2024. p. 45-50.

14. Громико І.О. Головний закон захисту інформації. VII Міжнародна науково-практична конференція “Theoretical and empirical scientific research: concept and trends”- Section XI Information technologies and systems – DOI 10.36074/logos-16.08.2024.001 – м. Оксфорд, Сполучене Королівство. 16 серпня 2024. p. 177-188.

15. Громико І.О. Пірамідальна модель доступу громадянина до державної таємниці. Збірник доповідей VI міжнародної науково-практичної конференції “Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи” 29 жовтня 2025 р./ Міністерство оборони України, НУОУ. УДК: 355.451 – К.: НУОУ, 2025. 237 с. – Ст.131-135.

Information about the authors:
Hromyko Ihor Oleksiyovych,
Candidate of Technical Sciences, Professor ZVO
of the Educational and Research Institute Computer Sciences
and Artificial Intelligence of Department of Security
of Information Systems, Networks & Technologies,
Associate Professor,
V. N. Karazin Kharkiv National University
6, Svobody Sq., Kharkiv, 61022, Ukraine
https://orcid.org/0000-0002-7701-9557