Берталанфи Л. фон. Общая теория систем: Критический обзор // Исследования по общей теории систем. М.: Прогресс, 1969 с. 23-82. ***10.*** *Кадомцев Б. Б. Динамика и самоорганизация. УФН. 164, №5, 4491994) – 396 с. 11. Бриллюен Л. Наука и теория информации. М.: Физматгиз, 1960.* ***12.*** *Кулик С. П. Физические основы квантовой информации. Лекции физ. фак. МГУ. http://qopt.phys.msu.su/speckurs/quantinf/lecture.pdf.* ***13.*** *Манойло С., Оскома Р. Квантовые вычисления. Алгоритмы эффективного решения NP-полных задач. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 11, К: 2005. С 153 - 157.* ***14.*** *Блюменфельд Л. А. Информация, термодинамика и конструкция биологических систем. // Соросовский образовательный журнал, № 7, 1996. – С. 88 – 92.* ***15.*** *Хакен Г. Информация и самоорганизация: Макроскопический подход к сложным системам: Пер. с англ.–М.: Мир, 1991. – 240 с.* ***16.*** *Боулдинг К. Общая теория систем - скелет науки // Исследования по общей теории систем. М.: Прогресс, 1969 с. 106-124.* ***17.*** *Стратонович Р . Л. Теория информации. – М.: Сов. Радио. 1975. – 424 с.* ***18.*** *Рамперсад К. Хьюберт. Универсальная система показателей деятельности: Как достигать результатов, сохраняя целостность / Пер. с англ. – М.: Альпина Бизнес Букс, 2005. – 352 с.*

УДК 681.321;322:621.395

ПАРАДИГМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕБІОМЕТРИКИ ТА СЕНСОРНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Володимир Кононович, Микола Тардаскін*

*Академія зв'язку України, *Одеський регіональний центр ТЗІ ВАТ "Укртелеком"*

Анотація: **Аналізуються аспекти захищеності та інформаційної безпеки телебіометрики і бездротових сенсорних мереж при взаємодії людей між собою та навколишнім середовищем з використанням моделі, рекомендованої міжнародним стандартом МСЕ-Т (Рекомендація Х.1081). Розглядається парадигма інформаційної безпеки нових інформаційних технологій.**

Summary: **Aspects of security both information safety of the telebiometric and Wireless Sensor Networks are analyzed at interaction of people among themselves and by an environment with use of the model recommended international standard (ITU-T Recommendation X.1081). The paradigm of information security of new information technologies is considered.**

Ключові слова: **Інформаційна безпека, захищеність, телекомунікаційні мережі, сенсорні мережі, телебіометрика, особиста сфера приватності, парадигма інформаційної безпеки.**

І Вступ

Розвинуте і стабільне інформаційне суспільство характеризується можливістю та спроможністю держави створювати умови для вільного доступу своїх громадян до інформаційних ресурсів, та умінням захищати національні інформаційні ресурси, інтереси особи, суспільства та держави в цілому від внутрішнього і зовнішнього негативного впливу [1]. При цьому, у сфері захисту інформаційних ресурсів необхідно забезпечувати надійне, безпечне функціонування національної інформаційної інфраструктури та її подальший ефективний розвиток. Існуюча парадигма класичного технічного захисту інформації полягає в забезпеченні збереження заданих властивостей інформації та інформаційно-телекомунікаційної системи, а саме: конфіденційності й цілісності інформації, доступності ресурсу системи, цілісності і спостережності інформаційно-телекомунікаційної системи [2]. Класична система технічного захисту інформації заснована, головним чином, на автономності і локальності інформаційних ресурсів інформаційної системи. Концепція захисту передбачала, як головні задачі, обмеження кола користувачів і створення системи розмежування доступу користувачів до інформації за категоріями.

З розширенням сфери застосування інформаційних технологій, глобальним розповсюдженням Інтернет, активним впровадженням доступу до розподілених баз даних за технологією клієнт - сервер з'являються операційні системи з багаторівневим захистом від несанкціонованого доступу, застосовується криптографія для шифрування транзакцій, впроваджуються засоби блокування підключення пристроїв. Має розповсюдження концептуальна технічна модель ешелонованої багаторівневої системи інформаційної безпеки міжнародного стандарту ISO/IEC 15408 [3], який визначає нову технологію розробки профілів захисту та проектів безпеки. Ряд фахівців пропонують впровадити цей стандарт в Україні [4], такий стандарт вже введений в Російській Федерації методом "обкладинки" [5]. Концептуальна модель системи інформаційної безпеки включає в себе набір послуг безпеки (та механізмів безпеки, які ці послуги реалізують), що забезпечують функції моніторингу, захисту та застосування інформаційних ресурсів з

метою поетапного запобігання можливості проникнення порушником, виявлення факту проникнення, локалізації об'єкта вторгнення й нападу, нейтралізації та видворення порушника, відновлення втрачених функцій системи. Новим у концептуальній моделі є широке застосування фільтрів, міжмережних екранів, систем виявлення атак та розпізнавання аномальної поведінки, адаптивних алгоритмів відновлення тощо.

Набутий досвід та наукові дослідження в цій галузі, а також бурхливий розвиток самих мереж змінюють парадигму захисту, в якій уточнюються і розширюються класичні критерії оцінки і стратегії забезпечення інформаційної безпеки. Розвивається концептуальний підхід «інформаційної гарантії» (information assurance) до захисту інформаційних ресурсів та нова «мережецентрична» парадигма інформаційної безпеки, якою інформаційна безпека напряму зв'язується з безпекою інфраструктури країни [6]. Ця парадигма є наслідком, перед усім, підвищених вимог до живучості інформаційних систем, які характеризуються високим ступенем розподілення ресурсів (технічної експлуатації та обслуговування, алгоритмів, програмного і апаратного забезпечення, телекомунікацій) і децентралізацією управління. Розвиток систем інформаційної безпеки проходить на фоні стрімкого розвитку й самого об'єкта захисту – інформаційно-телекомунікаційних технологій. В Україні завершується процес цифровізації телекомунікаційних мереж та інтеграції інформаційних і телекомунікаційних технологій, що виражається зокрема, в широкому вжитку в нормативно-правових документах нового терміну – «інформаційно-телекомунікаційні системи». В рамках реалізації проектів електронного суспільства створюються пакетні мультисервісні мережі телекомунікацій на єдиних принципах пакетного методу передачі мови, даних, зображень, відео тощо і побудованих на базі технологій мереж наступного покоління (NGN – Next Generic Network) [7]. Нові інформаційні і телекомунікаційні системи і технології створюються з урахуванням вимог інформаційної безпеки. Але процеси стандартизації системи інформаційної безпеки у NGN ще далекі від свого завершення.

Наступним витком конвергенції ресурсів і функцій мереж може бути створення широкосмугової поліфункціональної конвергентної мережі (BCN – Broadband convergence Network), в якій буде інтегроване також і телерадіомовлення, зокрема інтерактивне. BCN є спадкоємницею NGN. Технологічною основою BCN є транспортна мережа, заснована на базі протоколу IPv6. Одним з напрямів розвитку BCN, який є своєрідною реалізацією відомої теорії всепроникаючої комп'ютеризації, стають (також всепроникаючі) сенсорні мережі, що реалізують інтеграцію людини і комп'ютера у єдину мережу [8]. Поява таких мереж може суттєво змінити характеристики створюваного електронного суспільства. Тому інформаційна безпека сенсорних мереж та телебіометрики є сферою особливого піклування і предметом дослідження даної роботи. Деяким прообразом таких мереж сьогодні може служити радіочастотна ідентифікація об'єктів за технологією RFID (Radio Frequency Identification). Радіочастотна ідентифікація наділяє об'єкт (товар, продукт, багаж, документ тощо) інтелектом, надає йому можливість прямо спілкуватись з комп'ютером, а через нього з будь-яким учасником у процесі взаємодії [9]. Недоліком такої технології є все та ж недостатня інформаційна безпека й нові загрози, що супроводжують їх використання. Приміром є загроза простежування пристрастей споживача, необхідний захист від небажаного сканування і відстеження людей і майна, треба запобігати незаконному доступу небажаних осіб до важливої інформації.

Загальною рисою розвитку не лише інформаційних технологій, а й практично всіх технологій є надзвичайно висока ступінь їх інтеграції в усіх сферах людської діяльності і зумовленою цією обставиною взаємозалежністю і техногенною вразливістю, техногенними загрозами. Проблеми захисту всієї інфраструктури випливають із непередбачуваності наслідків кризисних ситуацій, зв'язаних з великомасштабними техногенними катастрофами на об'єктах інфраструктури. Незадовільною є ситуація, що склалась з інформаційною безпекою бездротового протоколу технології Bluetooth. Недостатньо захищеним залишається рухомий зв'язок. Взагалі, проблема захисту комунікацій, які вкрай залежні від інформаційних технологій і телекомунікаційної інфраструктури, стає ключовою для забезпечення ефективного функціонування всіх державних і суспільних інститутів практично в будь-якій країні світу.

Метою даної роботи є розробка основ та підходів до побудови моделі інформаційної безпеки систем телебіометрики і сенсорних мереж, які створюють комунікаційну основу телебіометричних систем.

Постановка задачі. Задача вирішується шляхом аналізу перспективної парадигми інформаційної безпеки нових інформаційних технологій, аспектів захищеності та інформаційної безпеки телебіометрики і сенсорних мереж при взаємодії людей між собою та з навколишнім середовищем з використанням моделі, рекомендованої міжнародним стандартом МСЕ (Рекомендація X.1081 [10]). Тим самим можна сприяти випереджаючим темпам розвитку систем інформаційної безпеки та, в ідеалі, досягти стану, коли спочатку створюється система інформаційної безпеки, а потім в неї вбудовується нова технологія, а не навпаки.

II Модель та аспекти інформаційної і фізичної захищеності телебіометнрики

Рекомендація X.1081 ITU-T надає мультимодальну модель телебіометрики (ММТ), яка включає

класифікації біометричних технологій, визначення і формування вимог до аспектів захищеності телебіометрики та вимоги до забезпечення її інформаційної й фізичної безпеки. Модель може бути застосована в сферах приватності, біометричної автентифікації, екологічної безпеки (ecological liability), і прийнятної біометричної схеми автентифікації, яка використовується для ідентифікації. ММТ була розвинута на основі теорії систем, градації шкал, ієрархії і засобів взаємодії між людиною і навколишнім середовищем, а також специфікацій ISO 31 і IEC 60027-1 щодо величин і одиниць для усіх відомих форм вимірювань величин фізичних взаємодій між людиною та її навколишнім середовищем.

Під приватністю розуміється право кожної людини-користувача телекомунікаційних послуг бути фізично захищеним й інформаційно безпечним при використанні телекомунікаційних терміналів. Додана цінність телекомунікаційних послуг полягає у тому, що значуща інформація доставляється в потрібний час, у відповідному контексті до сприймаючої людини-користувача, задовольняє деяку потребу і є фізично та інформаційно безпечна.

Людина розглядається у ММТ в термінах можливих взаємодій між цією людиною та її навколишнім середовищем як біосфера – сфера радіусом 1 м, що оточує персону. Якщо вона асоціюється із заходами забезпечення інформаційної й фізичної безпеки, то ця сфера називається особистою сферою індивідуального захисту (особистою сферою приватності – ОСП). Приватність людини-користувача може при мінімалістському підході базуватись на ОСП. Ця ОСП має природну середню тривалість, як біологічне явище, 3 000 000 000 с (приблизно 95 років).

ОСП – це фундаментальна відправна точка для абстракції людини в її взаємодії з навколишнім середовищем. Внутрішні процеси людини, як результат або реакції на такі взаємодії, не моделюються. Людина, як живий організм, моделюється як чорний ящик, який взаємодіє з її навколишнім середовищем в межах ОСП. Людина представляється як природна електронна система, яка може бути поділена на скалярні вектори і в якій необхідно задовольнити проблеми безпеки.

Перцептуальні, пізнавальні і моторні компоненти людського інтелекту привносяться у взаємовідносини з подібними компонентами іншої людини через технології телекомунікацій. Записи вимірювань, отриманих від людини, можуть бути використані з метою автентифікації, доказу ідентичності тощо. Екологічна безпека має забезпечуватись в домені антен, а безпека людини – в домені терміналів, пристроїв, які утримуються або функціонують в межах ОСП. Біометричні схеми автентифікації, які включають в себе телекомунікаційні можливості, повинні залишитись як вибір (опція використання) клієнтом телекомунікаційних послуг, забезпечувати досяжність, враховувати людські фактори і реалізовуватися етно-політично коректно.

ММТ – це модель з трьома рівнями: науковим, сенсорним і метричним. Науковий рівень визначає області академічних досліджень, застосовує різні дисципліни для дослідження взаємодій у ОСП. Для ММТ важливі такі наукові дисципліни, як фізика, хімія, біологія, культурологія і соціальні дисципліни, психологія. Взаємодії в ОСП можуть бути вивчені, використовуючи концепції і підходи багатьох різних дисциплін та їх комбінацій (біохімії, психофізики тощо). Кожна дисципліна вносить вклад у вивчення специфічних методів взаємодії, в розробку засобів ідентифікації, в специфікацію обмежень, гарантій та граничних величин, які можуть бути шкідливими, і так далі. ММТ передбачає дослідження взаємодій з точки зору кожної з важливих наукових дисциплін або їх комбінацій. ММТ може: допомогти з визначенням безпечних границь функціонування телекомунікаційних систем і біометричних пристроїв; забезпечити основу для розвитку таксономії біометричних пристроїв; сприяти розвитку автентифікаційних механізмів, заснованих на статичних (наприклад, відбитки пальця) і динамічних (наприклад, хода, або зміни тиску підпису) атрибутах справжньої людини.

Сенсорний рівень ММТ визначає взаємодії, які можуть класифікуватись за методами, за ідеальними типами та типами ознак взаємодії. До методів взаємодії належать основні відомі методи взаємодій: відео, аудіо, тактильні, хімічні та радіо. У ММТ розглядаються фізичні та поведінкові взаємодії. Останні поки що не визначені кількісними стандартними одиницями. Ідеальні типи взаємодії розділяють на поведінковий, перцептуальний та концептуальний ідеальний типи взаємодій. Поведінковий та перцептуальний типи притаманні всім основним методам взаємодії і визначають напрям взаємодії. Поведінковий тип представляє взаємодії від людини до навколишнього середовища. Перцептуальний, навпаки, представляє взаємодії від навколишнього середовища до людини. Концептуальний ідеальний тип взаємодії представляє знання, уявлення людини щодо навколишнього середовища і зв’язаний з обґрунтованою інформацією відносно безпеки. Концептуальний ідеальний тип взаємодії виражає: "Щось, що ми знаємо", приміром – паролі, PIN-коди, дівоча фамілія матері, дати народження.

Класифікація за типами ознак включає: постуральні (що відносяться до пози) – жестикуляційні; вербальні ознаки; ознаки, які відносяться до обличчя; до манери поведінки; та до взаємодії без прикмет. Ознаки, які спостерігаються у тіла людини вивчаються наукою semio-антропологією. Комбінації ознак

використовується з метою надлишковості (резервування) і для зняття протиріч значущої інформації. Вони адекватні політиці безпеки захисту користувачів, операторів телекомунікацій і провайдерів послуг з метою автентифікації. Відповідно до багаторівневого і мультимодального підходу телебіометрики мультимодальна досконала людина (чорний ящик) розміщена в межах структури ієрархічних шкал і охоплює перцептуальні, концептуальні и поведінкові фактори комунікацій. Виділені десять перцептуальних і поведінкових категорій: відео приймання (я бачу це), відео передача (це бачить мене), аудіо приймання (я чую це), аудіо передача (це чує мене), дотик цього (я торкаюсь цього), дотик мене (це торкається мене), хімічне приймання (я смакую або дегустую це), хімічна передача (це нюхає або пробує мене), радіо приймання (я опромінююсь), радіо передача (я випромінюю).

Метричний рівень ММТ визначає засоби вимірювань, шкали вимірювань, величини, використані у вимірюваннях, і посилається на сім базових одиниць СІ, даних у ISO 31, IEC 60027-1: m – довжина, kg – маса, s – час, A – електричний струм, K – термодинамічна температура, mol – молекулярна маса речовини, cd – інтенсивності люмінесценції. Модель складається із специфікації множини вимірювань, які забезпечують таксономію всіх можливих взаємодій, що складає більш ніж 1600 комбінацій одиниць вимірювань, виділених окремих методів і полів випромінювань.

У ОСП виділяються концентричні сфери близькості з біосфери користувача до систем телекомунікацій. Ці концентричні сфери одержані з десяти ступінчатого переліку найменувань метрологічних одиниць в ISO 31 і IEC 60027-1 і розглядаються як сектори, які будуть визначатись атрибутами, що дають верхні і нижні пороги для не шкідливих (безпечних) взаємодій з терміналами. Мультимодальність моделюється в межах структури ієрархії шкал, побудованій на основних і похідних одиницях СІ. В межах ММТ охоплюються чотири проблеми інформаційної безпеки: приватності (privacy), біометричної автенифікації (biometric authentication), фізичної безпеки (safety) і інформаційної безпеки (security). Незважаючи на очевидні відмінності, вони мають єдину послідовну обробку параметрів. На будь-якому рівні шкал і в будь-якій області спостерігач може зосередитись на визначенні набору верхніх і нижніх порогів, щоб гарантувати цілісність і підтримуваність (sustainability) ОСП.

Що стосується стандартизації біометричних пристроїв, то планується робота по стандартизації в напрямі біометричних типів (табл. 1).

Таблиця 1 – Біометричні типи та методи взаємодії

Біометричні типи	Модальність взаємодії (Interaction modality)
Образ обличчя, подробиці пальця, радужна оболонка, сітчатка, геометрія руки, зразки стилю, відбиток пальця.	Відео приймання і відео передача
Рухи губ, тепловий портрет обличчя, теплове зображення кисті руки, форма вушної раковини, геометрія пальця.	Відео передача
Аудіо, голос.	Аудіо передача
Динаміка підпису, динаміка натиснення клавіш, відбиток ноги.	Передача тактильних даних
Хода.	Поступальні дані (що відноситься до пози)
Запах тіла, ДНК	Хімічна видача
Подробиці пальця, відбиток кисті, модель пальця.	Залежить від використаної технології, відео або тактильні дані.

Сигнали, одержані на нижньому рівні біополя, яке надійно і захищено взаємодіє з телекомунікаційною системою, покидають далі біосферу. Керівними принципами на цьому етапі є: нешкідливість у наборі сигналів, які йдуть всередину біосфери від пристроїв телекомунікацій та повної доступності і автентифікованості (authenticability) в наборі сигналів, які йдуть у напрямі зовні від ОСП.

В цілому, людина, як живий об’єкт, моделюється як чорний ящик, який взаємодіє з навколишнім середовищем у межах ОСП на деякому рівні ієрархічних шкал та досяжності. При цьому вона створює виявлювані взаємодії з його навколишнім середовищем, які можуть бути використані для біометричної ідентифікації і автентифікації; може приймати і може потенційно бути пошкодженою взаємодіями, що надходять, а також має права і привілеї відносно як природи взаємодій, що надходять, так і використання результатів взаємодій.

III Архітектурні та функціональні особливості сенсорних комунікаційних мереж

ММТ охоплює можливі інформаційно і фізично безпечні мультимодальні людино-машинні взаємодії в

сфері телекомунікацій, включаючи пізнавальні, перцептуальні і поведінкові властивості людини, та застосовування біометричних сенсорів, або виконавчих елементів у майбутньому, з метою автентифікації. Біосфера самоорганізації ОСП – є само рухомою топологічною сферою (радіусом 1 м). Вона є суб'єктом обчислення, в якому живе світовий громадянин з бажаннями використання телекомунікаційних послуг та обладнання. Цей унікальний Einsteinian названий не підпорядкованою ОСП (Personal privacy sphere - PPS). Цілеспрямований і повністю захищений користувач телекомунікаційних мереж має унікальні біометричні ознаки, які сприймаються високо безпечними детекторами, зашифровуються в унікальний ідентифікатор і передаються за допомогою придатного для цього протоколу автентифікації. В унікальний ідентифікатор можуть бути включені (можливо отримані через глобальну систему позиціювання) ідентифікація і позначка часу, а також інші унікальні дані, які можуть бути необхідні для будь-якого бажаного рівня безпеки.

Мультимодальна телебіометрика практично реалізується сектором телекомунікацій, який названий сенсорними мережами. В архітектурі широкосмугової конвергентної мережі сенсорні мережі посідають рівень доступу (рис. 1). BCN як і NGN включає три рівні: рівень доступу, де забезпечується з'єднання термінального обладнання з транспортною телекомунікаційною мережею; рівень ядра мережі, яке забезпечує транспортування та розподіл інформації залежно від її адреси призначення, і яке реалізовано як транспортна мережа на базі протоколу IPv6; рівень серверів застосувань, які забезпечують послуги та управління мережею. Крім сенсорних мереж на рівні доступу архітектури BCN передбачаються: ТфМЗК – телефонна мережа загального користування, Інтернет, мобільні мережі, цифрове мультимедійне телерадіомовлення (DMB – Digital Multimedia Broadcasting). Можна очікувати, що ці мережі будуть реалізовані віртуально в деякій універсальній «телекомунікаційній матриці доступу».

Рисунок 1 – Архітектура широкосмугової конвергентної поліфункціональної телекомунікаційної мережі

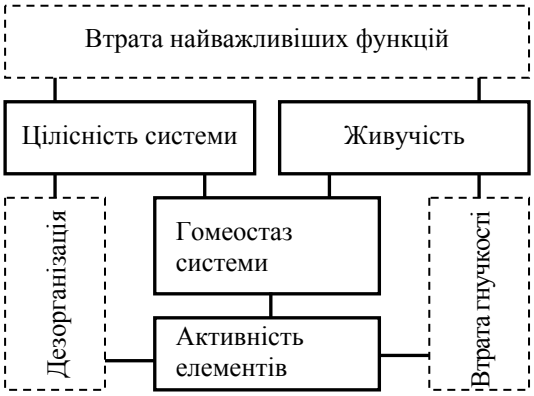

Рисунок 2 – Концептуальна модель гомеостазу відкритої інформаційної системи [6]

Бездротові сенсорні мережі (WSN – Wireless Sensor Networks) – це одна з перспективних технологій XXI століття [11], яка зв'язана з інтеграцією людини і комп'ютера у єдину мережу. Велика кількість сенсорів, об'єднаних у мережу, яка, в свою чергу, приєднана до глобальної телекомунікаційної мережі, нададуть широкі послуги з контролю і керуванню домами, підприємствами, транспортом, контролем за станом людей, забезпечення військових стратегій, керуванню кризовими і надзвичайними ситуаціями, боротьбою з тероризмом тощо. Сенсори, які носитиме людина, або які будуть імплантовані в її тіло чи вмонтовані у її оточення, дозволять контролювати життєдіяльність, причому при вільному пересуванні людини, й зокрема таку інформацію: індивідуальні фізичні дані, здоров'я, медичні показники; особисті характеристики; документальні дані – паспорт, індивідуальний податковий номер тощо; місцезнаходження, швидкість і вектор пересування; ідентифікацію особи при необхідності доступу до приміщень або ресурсів мережі.

Архітектуру сенсора складають: сам сенсорний пристрій, пам'ять, антена і джерело живлення. Сенсорні мережі зможуть відповідати таким вимогам: масштабованість при об'єднанні великої кількості (декілька десятків тисяч) сенсорів у мережу; мале споживання енергії при тому, що тривалість життя сенсора може бути обмежене тривалістю дії джерела живлення; самоорганізація мережі при виході з ладу елементів мережі або додаванні нових елементів. Сенсорні мережі можуть бути розгорнуті на землі, в повітрі, над і під водою. Самоорганізація мереж повинна забезпечуватись при випадковому і динамічному розташуванню на заданій території, при виході із ладу учасників мережі з різних причин, при необхідності

різко збільшити свою пропускну здатність, коли носії терміналів скупчуються в одному місці тощо. Сенсорні мережі мають мати певний інтелект. Вони забезпечують безперервне сканування терміналів біометрики, мають свої бази даних і передають центральному серверу лише зміни величин. Якщо термінал неактивний, то і потік інформації теж дорівнює нулю. Мережа має проектуватись як система, що саморозвивається, забезпечує свою гомеокінетичну рівновагу і функціонує як відкрита система з самоорганізацією, яка автоматично забезпечує підтримання гомеостазу системи (рис. 2).

Сенсорні мережі та телебіометрика можуть суттєво змінити існуючі характеристики суспільства. Включення сенсорних мереж до широкосмугової конвергентної мережі вимагає уважного відношення до проблем якості обслуговування (QoS), до інформаційної, фізичної й інших видів безпеки. Телекомунікаційні мережі повинні забезпечити виконання найбільш важливих задач навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні у контури керування, втраті частини ресурсів та перенавантаженні трафіка, частини ресурсів комплексу організаційно-технічних заходів захисту. Збої й відмови обладнання, перекручення та витік інформації, саботаж персоналу, шпигунство, дії хакерів, диверсії та терористичні акти на об'єктах інформаційної інфраструктури мають розглядатися як неминучі системотехнічні фактори навколишнього середовища. Для повноцінної роботи і збереження мінімального набору критично важливих функцій мережа повинна володіти цілком визначеним певним запасом стійкості до зовнішніх дестабілізуючих впливів середовища. При цьому порушення цілісності системи на фоні зниження активності її елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, зниження живучості та порушення цілісності системи – втрату найважливіших функцій [12]. Телекомунікаційні системи майбутнього повинні не тільки і не стільки обмежувати допуск користувачів до програм, даних і знань, скільки визначати і делегувати їх повноваження у корпоративному вирішенні задач, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації і усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів. Живучість інформаційно-телекомунікаційних систем набирає визначального значення для фізичної та інформаційної безпеки і визначає безпеку інфраструктури держави в цілому, готовність збройних сил, промисловості, економіки, народного господарства і суспільства як до ведення війни, так і до ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф.

IV Парадигма інформаційної безпеки сенсорних та телекомунікаційних мереж

Впровадження і розвиток телебіометрики та сенсорних мереж приведе до змін не лише у моральній і соціальній сфері та сфері суспільних відносин, не лише у підходах до національної, інформаційної, економічної і особистої безпеки, які мають бути уважно вивчені вже зараз. Змінюється суттєво і парадигма інформаційної безпеки телекомунікаційної системи, в яку входять сенсорні мережі. Незважаючи на своє вирішальне значення для розвитку інформаційного суспільства, інформаційно-комунікаційні технології (ІКТ) виявилися слабо захищеними від зловживань, потерпають від внутрішніх інцидентів, зв'язаних з порушенням персоналом регламенту використання інформаційних ресурсів, від зовнішніх вторгнень, стали ареною діяльності організованих кіберзлочинців, зокрема міжнародних, і розквіту кібертероризму. Статистика, наприклад, центру оперативного реагування CERT, свідчить, що темпи зростання кількості інцидентів з інформаційною безпекою продовжують зростати (рис. 3). В той же час, заходи протидії не встигають за ростом числа інцидентів. Кількість виявлених вразливостей у системах захисту стабілізувалось на рівні 4000 за рік (рис. 4), що свідчить про досягнення граничної продуктивності праці колективів програмістів, які розробляють закриті програмні продукти для інформаційних систем. Поки що у класичному протистоянні злочинності і суспільства в галузі ІКТ виграють злочинці. Суспільство не може миритись із ситуацією з інформаційною безпекою, що склалася сьогодні.

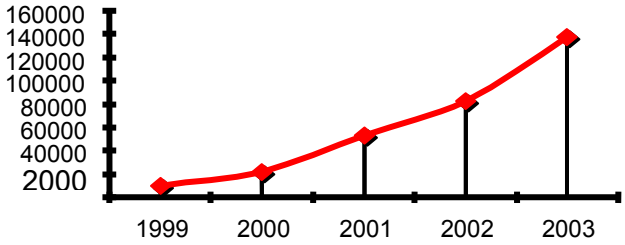

Рисунок 3 – Кількість інцидентів з інформаційною безпекою

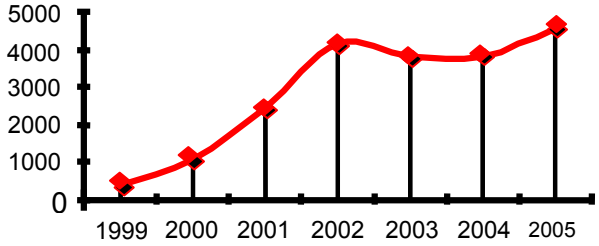

Рисунок 4 – Кількість виявлених вразливостей

Сучасний порядок побудови і використання системи інформаційної безпеки (СІБ), що став класичним і охоплює всі етапи життєвого циклу СІБ, може бути описаний алгоритмом, який показано на рис. 5. Його етапи описані у відповідних нормативних документах системи технічного захисту інформації. Новим тут є лише те, що алгоритм можна умовно поділити на глобальну і локальну частини, а саме – на частину за часом розробки і частину за часом використання. Глобальна частина (частина за часом розробки) закінчується прийняттям системи в експлуатацію, а локальна частина (за часом використання) охоплює собою етапи, які реалізуються протягом технічної експлуатації СІБ. Циклічність алгоритму в локальній його частині є принципово необхідною. При зменшенні рівня захищеності або виявленні нових загроз, що виникли під час експлуатації, а також при змінах та при вдосконаленні самої ІКТ має бути прийняте рішення про доробку чи вдосконалення СІБ. Тоді й виникають цикли повторення етапів локальної частини алгоритму: розробки локального ТЗ або технічних умов (ТУ) на вдосконалення СІБ та змін політики безпеки; проектування вдосконалень у СІБ; втілення вдосконалень у діючу СІБ та змін у політиці безпеки; тестування вдосконаленої СІБ; повторної державної експертизи СІБ у встановленому порядку та продовження експлуатації до етапу планового виведення СІБ з експлуатації та її утилізації. Цю частину алгоритму можна назвати алгоритмом вдосконалення СІБ, який є циклічним і має вигляд як на рис. 6.

На етапі експлуатації СІБ політикою безпеки передбачається проведення моніторингу інформаційної безпеки, управління інформаційною безпекою, аудиту та інших заходів, які забезпечують контроль стану і рівня захищеності інформаційних ресурсів та виявлення нових загроз.

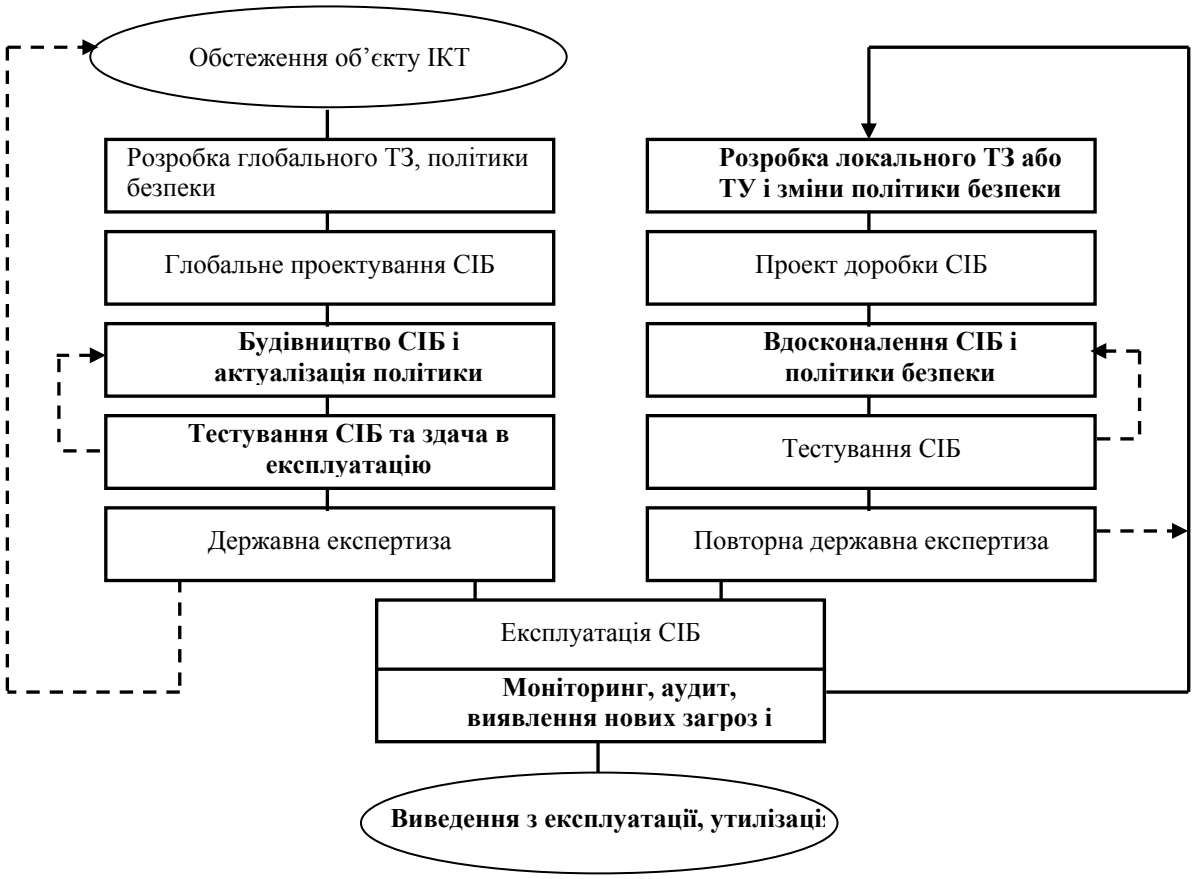

Рисунок 5 – Порядок побудови і використання системи інформаційної безпеки

Недоліки у області інформаційної безпеки (ІБ) можна поділити на: загальні; недоліки роботи з персоналом; та невідповідність класичної парадигми ІБ новому рівню розвитку ІКТ. До загальних недоліків відносяться: епізодична, від випадку до випадку, увага з боку керівництва до даної проблеми; відсутність стрункої, збалансованої системи критеріїв ефективності, слаба система професійної підготовки і навчання, неефективна інвестиційна політика, слабий контроль за ІБ на стадії складання контрактів на постачання інформаційних технологій; відсутність на місцях систем виявлення вторгнень і недостатній обмін інформацією та недостатня увага до збору статистики, яка стосується ІБ.

Рисунок 6 – Алгоритм вдосконалення системи інформаційної безпеки

Проблеми, зв'язані з підготовкою персоналу у області ІБ: недостача кваліфікованого персоналу; мала середня заробітна плата фахівців старшої і середньої ланки; неефективна система підбору кадрів на посади фахівців у області ІБ; слаба мотивація для професійного росту фахівців у області ІБ; недосконала система після вузівського навчання, система професійної і тарифної класифікації застаріла і відображає модель постіндустріального суспільства.

Стають зрозумілими деякі недоліки класичного підходу до інформаційної безпеки та процесу створення і використання СІБ. По-перше, процес створення СІБ починається надто пізно. У багатьох випадках спочатку створюється ІКТ без обґрунтованого врахування вимог до інформаційної безпеки, а потім, після отримання збитків внаслідок здійснених порушень, або загроз порушень інформаційної безпеки, приймається рішення про створення СІБ. У результаті створюється ІКТ, яким притаманні різні вразливості, слабкі місця. Зловмисники, в решті решт, ці вразливості виявляють і негайно використовують для проникнення. СІБ у цих умовах має нейтралізувати (залатати) усі наявні вразливості. В сучасних ІКТ можна виділити такі види вразливостей і слабких місць: природжені, зумовлені властивостями самої технології; привнесені внаслідок помилок в програмно-апаратному забезпеченні, або низької якості виконання, або апаратної чи логічної (якісної) недостатності (наприклад, завищеною імовірністю перенавантаження); навмисне закладені; випадкові. Привнесені, випадкові і навмисне закладені вразливості виявляються при обстеженні або експертизі СІБ. При великій складності сучасних систем залишається значна кількість невиявлених помилок у програмному забезпеченні і навіть у проектних рішеннях. Тому ці вразливості продовжують виявлятись під час експлуатації систем.

Що стосується природжених вразливостей, то для боротьби з ними потрібні принципово інші рішення. Систему інформаційної безпеки доцільно створювати до, або разом зі створенням інформаційно-комунікаційної системи. Найбільш краще рішення проблеми інформаційної безпеки – це розробити і використовувати лише безпечні ІКТ. Слід зауважити, що в цьому напрямі йде напружена теоретична і практична робота. Створюються захищені комп'ютери і комп'ютерні системи, цифрові вузли комутації поставляються з вбудованими штатними системами захисту інформації, інженерні засоби захисту створюються ще під час будівництва споруд, інтенсивно просувається міжнародна стандартизація інформаційної безпеки нових систем телекомунікацій тощо. ММТ може бути використана, щоб забезпечити специфікації, зв'язані з проблемами фізичної захищеності, інформаційної безпеки, біометричної автентифікації і приватності. Але є і протилежні приклади. Новий протокол бездротового доступу технології Bluetooth виявився катастрофічно незахищеним.

Підсумовуючи сказане, приходимо до висновку, що замість ІКТ з умовною захищеністю, в яких залишається з деякою імовірністю певний процент помилок і вразливостей, необхідно розробити ІКТ з безумовною (інформаційно-теоретичною) стійкістю [13]. Інакше зростаюча кількість інцидентів з інформаційною безпекою може стабілізуватись на закритичному рівні, коли реальне використання ІКТ стане вже неможливим.

По друге, класичний підхід до інформаційної безпеки важко застосовувати до сучасних складних і надскладних інформаційних систем, які до того ж, безперервно розвиваються. Складну систему доводиться поділяти або на ієрархічні рівні і/або на більш прості системи і застосовувати класичну процедуру створення СІБ для кожної системи окремо. При цьому виникає загроза порушення основного теоретичного положення інформаційної безпеки складної системи, а саме – безперервності захисту у часі (за етапами життєвого циклу), просторі (за елементами мережі) і множині загроз (та вразливостей і слабких місць). Відомо, що рівень захищеності системи визначається найменш захищеною ланкою і не може бути вищим рівня захищеності цієї ланки. Така ж загроза виникає у порівняно нескладних ситуаціях

взаємодії декількох суб'єктів відносин, при яких використовуються ІКТ. Кожен з партнерів у часі підготовки і процесу взаємодії обробляє певний обсяг інформації, частина якої стає спільною і використовує певні інформаційні ресурси. Кожен з партнерів повинен забезпечити необхідний (базовий) рівень інформаційної безпеки, контрольований незалежним органом. Цей рівень має бути забезпечений однаковим як для власних, так і для спільних ресурсів. Будь-який власний ресурс може стати спільним і навпаки. При витоку інформації втрати можуть понести усі партнери, хоча несанкціонований витік інформації допущений лише в одному місці. Хоча в даному випадку витік інформації може допустити нечесний партнер-зловмисник.

Щоб стабілізувати рівень злочинності в ІКТ, доцільно забезпечити всіма суб'єктами взаємовідносин однаковий рівень інформаційної безпеки, не нижчий деякого базового. Встановлювати рівень інформаційної безпеки значно вищим, ніж базовий, при взаємодії з іншими учасниками, недоцільно, бо результуюча захищеність все одно не буде вище базового рівня. В умовах руху країни до інформаційного суспільства, забезпечення базового рівня інформаційної безпеки всіх без винятку суб'єктів інформаційних відносин та безпеки інформаційних ресурсів стає загально державною задачею, від вирішення якої залежить безпека, ефективність і надійність ІКТ. Всі суб'єкти взаємовідносин в державі повинні нести певні витрати на забезпечення інформаційної безпеки. Безпека ІКТ має забезпечуватись на державному рівні, подібно системі пожежної безпеки. Як і в системі пожежної безпеки, у сфері інформаційних відносин невживання заходів забезпечення інформаційної безпеки слід вважати економічним злочином. Повинні бути створені умови для того, щоб було економічно вигідно захищати інформацію як свою, так і партнерів з інформаційних взаємовідносин, так і споживачів телекомунікаційних послуг.

Чим вищий буде базовий рівень інформаційної безпеки на всіх об'єктах інформаційної діяльності, тим на нижчому рівні стабілізується кількість злочинів. Повністю ліквідувати злочинність не можливо. З психологічних досліджень відомо, що 10 – 15 % людей не скоять злочину ні при яких обставинах. Але є й 5 – 10 % людей, які будуть намагатись скоїти злочин, навіть усвідомлюючи невідворотність покарання. Ці люди будуть наполегливо шукати і штучно створювати вразливості ІКТ, щоб їх використати в своїх злочинних цілях. СІБ, як і правоохоронні органи, повинні планомірно і надійно залатати всі «дірки», вразливості і слабкі місця в інформаційній безпеці ІКТ.

По третє, ефективність створеної СІБ залежить, в значній мірі, від якості проведення початкових етапів – результатів обстеження об'єкту ІКТ, формування вимог до СІБ і, особливо – від оцінки цінності інформації та інших інформаційних ресурсів, які підлягають захисту. Класичний підхід до побудови СІБ передбачає попереднє визначення цінності інформаційних ресурсів та необхідного рівня їх захищеності. Початкові етапи є важливими, але й найбільш неоднозначними, частково невизначеними, нечіткими, суб'єктивними, а тому є слабким місцем класичного підходу до інформаційної безпеки. Цей недолік зв'язаний з недосконалістю нинішніх уявлень про цінність інформації. Саме поняття інформації ще не осмислено остаточно ні у філософському, ні в науково-прикладному планах. Достатньо обґрунтованих критеріїв цінності інформації поки що не знайдено. Теоретичні критерії Хартлі, Шенона, Харкевича, Колмогорова тощо відносяться до випадків статистичної цінності інформації і в практиці обробки реальної інформації їх застосовувати важко. Одним із методів визначення цінності інформації є розрахунки величини збитку внаслідок реалізації загроз, або розрахунки початкових ризиків інформаційної безпеки. Ці та інші практичні методи характеризуються такими особливостями: засобами обробки інформації є інша інформація (програми) і підходи до оцінки різних видів інформації можуть бути різними; одні види інформації можна оцінити кількісно, іншу лише якісно, застосовуючи неякісні шкали та експертні методи оцінки; кожен вид інформації може оцінюватись багатосторонньо. За одними критеріями цінність інформації може бути більшою, за іншими – меншою. На етапі розробки заходів захисту для кожного з елементів ІКТ обирають конкретні функціональні профілі захисту з послугами і механізмами безпеки, які мають забезпечити необхідні рівні захищеності. Знаючи вартість елементарних послуг та механізмів захисту можна визначити витрати на створення СІБ. При цьому недоліки попередніх етапів впливають на цей та наступні етапи, знижуючи рівень обґрунтованості прийнятих рішень.

Для усунення вказаного недоліку пропонується новий підхід до інформаційної безпеки, який має преваги в тому, що виключає необхідність безпосередньої оцінки цінності інформаційних ресурсів, і заміняє цю оцінку процедурою, яка характеризується меншим степенем невизначеності. Суть підходу полягає в тому, що для складних систем, із великою кількістю потоків інформації різних категорій, спочатку визначається доля витрат на інформаційну безпеку. Величина цієї долі витрат залежить від необхідного рівня захищеності і визначається на базі теорії і за аналогією з розподілом витрат у практично реалізованих СІБ. На сьогодні в середньому витрати на інформаційну безпеку становлять 10 – 15 % від загальних витрат. При цьому, чим більший обсяг капіталу чи обороту, тим більша доля витрат на інформаційну безпеку. Відомо, що конфіденційність інформації має тенденцію до підвищення при

збільшенні обсягів цієї інформації (даних).

Виділивши необхідну долю витрат на інформаційну безпеку всієї ІКТ, проводять розподіл їх за окремими об'єктами ІКТ, враховуючи їх критичність з точки зору захисту інформації. Далі на кожному з об'єктів застосовують класичні процедури створення СІБ (рис. 5) з метою ефективної побудови СІБ при заданих ресурсах. В результаті побудови СІБ буде реалізований певний (імовірно достатній) рівень захищеності інформаційних ресурсів і буде деякий залишковий ризик. Обмежені кошти не дають можливості досягти абсолютного захисту. Це неможливо й теоретично. СІБ знижує початковий ризик інформаційної безпеки до певного залишкового рівня. Для підвищення ефективності такого рішення застосовується страхування залишкових ризиків інформаційної безпеки.

Новий підхід до інформаційної безпеки обгрунтовується такими міркуваннями. Доля витрат на інформаційну безпеку може бути інтегральним показником рівня захищеності інформаційних ресурсів, якщо розрахувати їх за єдиною спеціальною методикою. Особливість цієї методики полягає в тому, що виділена доля витрат (приміром 20 %) далі оптимально розподіляється за етапами і забезпечується оптимальне використання виділених коштів для побудови СІБ. У окремих випадках витрати можуть розподілятись рівномірно за елементами мережі та за етапами життєвого циклу СІБ. Новий підхід частково компенсує недосконаліть нинішніх уявлень про цінність інформації. Замість безпосереднього визначення цінності інформації вона враховується опосередковано через її роль у бізнес-процесах, у створенні товарів, послуг, нової інформації, яка створена за її участі. Тобто цінність використовуваної інформації враховується, так би мовити, за результатами її використання.

Новий підхід не заперечує і не відміняє класичний, а застосовуються у випадках складних ІКТ та наявності багатьох взаємодіючих об'єктів. Новий підхід застосовується для визначення витрат на ІБ комплексно для всієї складної ІКТ, яка використовується взаємодіючими об'єктами. Після розподілу витрат по об'єктам застосовується класичний підхід, дещо скоригований, для створення СІБ на кожному з взаємодіючих об'єктів.

Висновки

1 Широке впровадження телебіометрики та сенсорних мереж неодмінно приведе до суттєвих змін у моральній і соціальній сферах та сфері суспільних відносин, у підходах до національної, інформаційної, економічної і особистої безпеки, які мають бути уважно вивчені вже зараз. Крім того, буде змінюватиси парадигма інформаційної безпеки телекомунікаційної системи, в яку входять сенсорні мережі.

2 Мультимодальна модель телебіометрики може бути використана, щоб забезпечити специфікації, зв'язані з проблемами фізичної захищеності, інформаційної безпеки, біометричної автентифікації і приватності.

3 Інформаційна безпека інформаційно-телекомунікаційних систем напряму зв'язується з живучістю інфраструктури телекомунікаційних мереж.

4 Технічна надійність, стійкість до збоїв, живучість інформаційно-телекомунікаційних мереж набирає визначального значення для фізичної та інформаційної безпеки і стає однією з характеристик системи інформаційної безпеки, визначаючи безпеку інфраструктури держави в цілому.

5 Обгрунтовані положення парадигми інформаційної безпеки у напрямі: змін у порядку побудови і використання системи інформаційної безпеки; введення етапів глобального (одночасного або раніше з розробкою самої інформаційної технології) та локального проектування системи інформаційної безпеки; впровадження нового підходу до розподілу витрат на систему інформаційної безпеки, який виключає етап важко здійснюваної оцінки цінності інформаційних ресурсів, і замінює цю оцінку процедурою, яка характеризується меншим степенем невизначеності; класична процедура створення системи інформаційної безпеки має застосовуватись, як і раніше, для створення комплексної системи захисту інформації на кожному окремому об'єкті з метою досягнення максимальної ефективності заздалегідь виділених коштів.

6 Відносно нової парадигми інформаційної безпеки інформаційно-телекомунікаційних мереж встановлено, що: необхідно забезпечити базовий (можливо однаковий) рівень безпеки всіх суб'єктів і об'єктів взаємодії, які використовують ІКТ; незахист інформації – тобто неприйняття заходів забезпечення базового рівня інформаційної безпеки – слід розглядати як злочин проти суспільства.

7 Стало життєво необхідним вирішення задачі розробки інформаційно-комунікаційних технологій з безумовною інформаційно-теоретичною стійкістю замість ІКТ з умовною захищеністю, в яких залишається з деякою імовірністю певний процент помилок і вразливостей;

Напрямами подальшої роботи є вдосконалення запропонованих методів вирішення нових проблем інформаційної безпеки інформаційно-телекомунікаційних мереж, розробка критеріїв оцінки та власне оцінка їх ефективності.

Література: ***1.*** *Бойко К. В. „Безпека сучасних інформаційних і телекомунікаційних мереж". // Доповідь на II міжнародній науково-практичній конференції,. Бизнес и безопасность, № 5, 2005. – С. 101-102.* ***2.*** *НД ТЗІ 1. 1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України, київ, 1999. – 24 с.* ***3.*** *Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model. – Part 2: Security functional requirements. – Part 3: Security assurance requirements.* ***4.*** *Бондаренко М., Скрыпник Л., Потий А. Перспективы применения международного стандарта ISO/IEC в Украине. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 3, 2001. С 7 – 26.* ***5.*** *ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности. Часть 3. Требования доверия к безопасности.– М.: ИПК Издательство стандартов, 2002.* ***6.*** *Леваков А. Анатомия информационной безопасности США. Jet Info online № 6(109), 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – 74 с.* ***7.*** *Кучерявий А. Е., Кучерявий Е. А. От Е-России к U-России: Тенденции развития электросвязи // Электросвязь, №5, 2005. С. 10 – 12.* ***8.*** *Weiser M. Hot Topic: Ubiquitous computing // IEEE computing. – October 1993.* ***9.*** *Мусієнко Д. Радіочастотна ідентифікація. // Бизнес и безопасность, № 5, 2005. – С. 29 – 33.* ***10.*** *ITU-T Recommendation X. 1081. The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics. – 22 с.* ***11.*** *21ideas for 21st century. // Busines Week. – August, 30, 1999.* ***12.*** *Modeling the Revolution in Military Affairs, Autumn/Winter 1998-99 / JFQ.* ***13.*** *Горицький В. М. Сучасний стан і перспективи розвитку інформаційного суспільства в Україні. // II науково-практична конференція «Безпека інформаційно-комунікаційних технологій». Діпрозв'язок, Київ , 2005. – 8 с.*

УДК 34+002

СТРАТЕГІЯ ФОРМУВАННЯ І РОЗВИТКУ ЗАХИЩЕНОГО СЕРВІСУ В ЕЛЕКТРОННИХ СИСТЕМАХ ПРАВОВОЇ ІНФОРМАЦІЇ

Валентин Венедіктов, Микола Логвиненко, Володимир Торяник
Харківський національний університет внутрішніх справ

Анотація. **Проаналізовано стан і основні тенденції розвитку електронних систем правової інформації. Поставлено завдання формування і структуризації необхідного інформаційного сервісу в цій сфері. Запропоновані технології розробки архітектур систем правової інформації, їх основних функцій і задач. Розроблено стратегію переходу до перспективних систем правової інформації на основі парадигми інтелектуального інформаційного сервісу, що радить.**
Summary: **The state and basic tendencies of development of the electronic systems of juridical information were analyzed. The task of forming and structuring of necessary informative service in this sphere was put. The technologies of development of the systems architecture of juridical information, their basic functions and tasks were offered. The strategy of turning to the perspective systems of juridical information based on the intellectual informative service paradigm, that advises, was developed.**
Ключові слова: **Правова інформатика, системи правової інформації, парадигма інтелектуального сервісу, що радить, інформаційна безпека.**

Вступ

Відомо, що ефективність діяльності держави визначається досконалістю її управління. Стрімкий розвиток інформаційних технологій відкрив нові можливості в усіх галузях економічної і соціальної діяльності. Необхідність і неминучість глобальної інформатизації загальновизнана [1 – 3]. Стратегічно важливою складовою інформатизації держави є правова інформатизація. Вона може об'єднати складові правової системи і здійснювати їх взаємодію на принципово нових засадах – за допомогою інформаційних технологій. Правова інформатизація стає одним з найважливіших напрямів розвитку державного управління [4].

Наукова основа правової інформатизації – правова інформатика, предметом якої є дослідження