С. 67 – 71. 4. Мерабишвили П.Ф., Вадачкория Г.В. Анализ динамики мостовых выпрямителей при синусоидальном токе на входе // Электричество. – 1992. – № 2. – С. 30 – 35. 5. Самотий В.В. Аналіз стаціонарних режимів трифазних однопівперіодних випрямлячів методом Ньютона // Вимірювальна техніка та метрологія: міжвідомчий наук.-техн. зб. – Львів, 1996. Вип. 52. – С. 95 – 97. 6. Самотий В.В., Гаранюк П.І. Математична модель трифазно-однофазного перетворювача частоти при активно-ємнісному навантаженні // Доповіді Національної академії наук України. – 1997. – № 11. – С.38–42. 7. Самотий В.В. Математичне моделювання стаціонарних процесів електромагнетних пристроїв систем керування. – Львів: Фенікс, 1997. – 170 с. 8. McLeod. A note on the e-algorithm // Computing (Areh. Electron. Rechnen). – 1971. – V. 7. – P. 17–24. 9. Samotyj W., Dzelendziak U., Chomulak M. Optymalizacja kształtu sygnału wyjściowego falownika tyrystorowego // V Ogólnopolska konferencja naukowo-techniczna Postępy w Elektrotechnice Stosowanej (PES-5). – T. II. – Kościelisko (Polska). – 2005. – S. 69 – 76.

УДК 004.7

В.Б. Дудикевич[1], Ю.Р. Гарасим[1], Г.В. Микитин[1, 2]
[1]Національний університет "Львівська політехніка",
кафедра захисту інформації;
[2]Фізико-механічний інститут ім. Г.В. Карпенка

КОНЦЕПТУАЛЬНІ МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ТЕХНОЛОГІЙ СТАЦІОНАРНОГО, СТІЛЬНИКОВОГО, СУПУТНИКОВОГО ЗВ'ЯЗКУ

Розроблено концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку на фізичному, канальному, мережевому, системному рівнях. Відповідно до запропонованої моделі проаналізовано аспекти захисту інформації в корпоративних мережах.

The conceptual models of information security for fixed, cellular, satellite communication technologies on physical, data link, network and system level were designed. Within the suggested model enterprise networks information security aspect were examined.

Вступ. Створення сучасних систем безпеки інформації, зокрема на рівні корпоративних мереж зв'язку (КМЗ), які є провідними в сучасній інфраструктурі функціонування суспільства, ґрунтується на комплексному підході, що охоплює принципи системного аналізу предметної сфери. Структура комплексного підходу орієнтована на створення захищеного середовища оброблення інформації на основі методів і засобів протидії відповідним загрозам. Методологічною основою комплексного підходу є: законодавчі, нормативно-правові, морально-етичні, організаційні, апаратно-програмні способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.

Комплексний підхід ефективно використовується в сучасних концепціях інформаційної безпеки засобів передавання/приймання сигналів, фізичних каналів і мереж зв'язку. Принципи побудови інформаційної безпеки цифрової системи зв'язку (ЦСЗ) ґрунтуються на:

– концептуальній моделі захисту інформації для відповідної технології зв'язку з урахуванням аспектів передавання/приймання фізичного сигналу, самого фізичного середовища – каналу, мережі, апаратно-програмних засобів цифрових систем зв'язку;

– адекватній математичній моделі сигналу (каналу), в якій закладено параметри якісного і кількісного рівнів взаємозв'язку вхідного і вихідного сигналу.

Взаємозв'язок параметрів математичної моделі сигналу відображає якісний рівень таких процедур перетворення сигналу ЦСЗ, як: форматування (дискретизація, квантування), кодування джерела, шифрування/дешифрування, кодування/декодування сигналу, імпульсна модуляція/демодуляція, фільтрація сигналів. Такі процедури впливають на швидкість передавання інформації, рівень захищеності інформації в каналах (мережах) зв'язку.

Синтез двох моделей цілісно відображає якісний і кількісний рівень захисту інформації для відповідної технології зв'язку та уможливлює створення відповідних методологій і підходів до ефективного захисту передавання/приймання інформації каналами і мережами зв'язку.

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ТЕХНОЛОГІЙ СТАЦІОНАРНОГО ЗВ'ЯЗКУ

Для створення концептуальної моделі (КМ) в роботі використано принципи системного аналізу – принцип ієрархічності (захист інформації розглядається з позиції: фізичного рівня – рівня сигналів, канального, мережевого та системного рівнів), принцип багатоаспектності – наведено кілька технологій зв'язку з метою аналізу якісного рівня захищеності процедури передавання/приймання інформації), принцип цілісності – охоплює кілька видів зв'язку, представлених окремими технологіями, що утворюють системну картину якісного рівня захисту інформації в каналах, мережах та системах зв'язку). На рис. 1 зображено концептуальну модель захисту інформації для технологій стаціонарного зв'язку.

Телефонні мережі загального користування: PSTN. Відповідно до процедури прямого та оберненого перетворення при передаванні/прийманні інформації в каналах зв'язку розглядаються такі ***технології захисту інформації*** (кожна технологія представляється методами та засобами захисту інформації): дискретизація з подальшим шифруванням/дешифруванням, скремблювання, канальне кодування/декодування, імпульсна модуляція/демодуляція, ущільнення/розущільнення, системи контролю доступу до обладнання АТС.

Методи захисту інформації: контроль нормалізованих параметрів лінії (імпедансу, напруги, струму); контроль сигналів у лінії (мовного та позамовного діапазону частот); рефлектометрія; активні та пасивні методи захисту телефонного тракту (обмеження небезпечних сигналів, фільтрування небезпечних сигналів, відмикання джерел небезпечних сигналів, метод високочастотної/низькочастотної маскувальної завади, метод ультразвукової маскувальної завади, метод "обнулення", компенсаційний метод, метод "випалювання"); обмеження фізичного доступу до лінії зв'язку; методи перетворення мовного сигналу.

Засоби захисту інформації: пристрої "Аккорд-200", "Хмара", "Барьер-3", "КТЛ-3", "КТЛ-400", Winkelman Model – 200, ТСМ-03, ТПУ-5, ТПУ-6, SP-18/T "Багер-01", багатофункціональний пристрій ST 031 "Пиранья", універсальний пошуковий пристрій Д-008, пошукові комплекси СРМ-700 "Акула" та системи Р5-1А, Р5-5, Р5-8 [1].

Технологія глобальних мереж: X.25, ISDN, ATM, Frame Relay. ***Технології захисту інформації***: шифрування/дешифрування, канальне кодування/декодування, імпульсна модуляція/демодуляція, маскування, ущільнення/розущільнення, системи контролю доступу до обладнання АТС, взаємна автентифікація, вставлення фіктивних повідомлень, доповнення повідомлень, постійний контроль роботи системи, адміністрування функцій та прав доступу.

Методи захисту інформації: реалізація у межах однієї системи різних рівнів захищеності для різних об'єктів захисту, реалізація у межах однієї системи різних функціональних профілів захищеності об'єктів (охоплюючи рівень якості конфіденційності, цілісності, доступності інформації та ресурсів, а також спостережуваності системи), динамічна адаптація системи захисту інформації (СЗІ) під змінні умови об'єктів захисту, її кількісний та якісний розвиток відповідно до змін моделі загроз, сертифікація (атестація або експертиза) СЗІ для системи зв'язку загалом, протоколювання та моніторинг подій, екранування приміщень, обмеження фізичного доступу до лінії зв'язку.

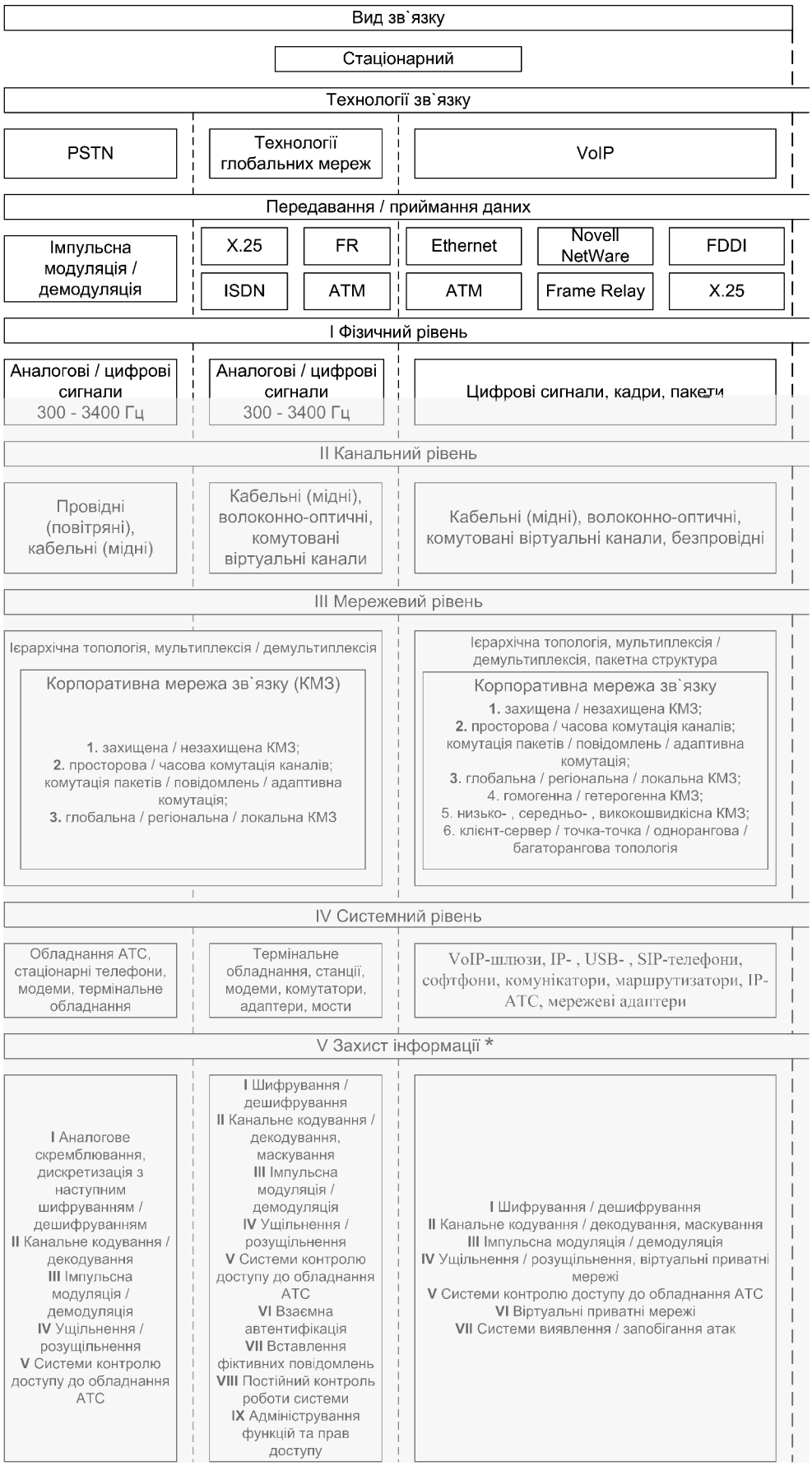

Рис. 1. Концептуальна модель захисту інформації для технологій стаціонарного зв'язку
**На схемі наведені лише технології захисту інформації, методи та засоби – у тексті статті*

Засоби захисту інформації: пункт контролю та управління зв'язком, засоби розмежування доступу, системи автоматичного нагляду, програми-аналізатори "аномалій", шифратори, IPSec [2].

IP-телефонія VoIP: Ethernet, ATM, Novell NetWare, Frame Relay, FDDI, X.25. ***Технології захисту інформації***: шифрування/дешифрування, канальне кодування/декодування, імпульсна модуляція/демодуляція, ущільнення/розущільнення, віртуальні приватні мережі, системи виявлення/запобігання атакам, системи контролю доступу до обладнання АТС.

Методи захисту інформації: криптографія, цифровий підпис, контроль цілісності системи, моніторинг журналів та систем-пасток [3].

Засоби захисту інформації: шифратори (DES, 3DES, AES, RC4), системи виявлення/запобігання атакам (NIDS – комерційні: Anzen Flight Jacket (AFJ), Cross-Site for Security, Net Prowler, NetRanger, SecureNet PRO, Session Wall-3, freeware: Shadow, Hummer, MOM, AAFID, Network Flight Recorder (NFR); HIDS – комерційні: Computer Misuse detection System (CMDS), CyberCop Monitor (CCM), Intruder Alert (ITA), Kane Security Monitor (KSM), SMARTWatch System Integrity Checker, freeware: HostSentry, Tripwire; гібридні IDS – Real Secure, Centrax), брандмауери, файрволи, захищені мережеві протоколи (на прикладному рівні SHTTP, S/MIME, PGP, SSH; на сеансовому рівні SOCKS, SSL/TLS; на сеансовому рівні IPSec, SKIP; на канальному рівні PPTP, L2TP), міжмережеві екрани – WatchGuard Firebox II, Firebox II Plus, Firebox II Fast VPN, системи-приманки – CyberCop Sting, системи контролю цілісності, цифровий підпис – RSA, DSA, ECDSA.

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ТЕХНОЛОГІЙ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Стандарти цифрового стільникового зв'язку в Європі, США та Японії: GSM, ADS (D-AMPS), JDS

Технології захисту інформації: автентифікація повідомлень, верифікація, біометрія, шифрування/дешифрування (криптомодулі), зміна частот зі зміною місця, передавання пакетів на різних частотах, системи контролю доступу до базової станції, шумоподібний сигнал з кодовим доступом, канальне кодування/декодування, скремблювання.

Методи захисту інформації: логін/пароль користувача, стратегія ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи, коди автентифікації, шифрування (RSA), секретність абонента, секретність передавання даних, секретність напрямів з'єднання абонентів, забезпечення цілісності, обмеження доступу до центрального вузла, управління роботою мережі та контроль цієї роботи, забезпечення резервних каналів, забезпечення конфіденційності на канальному та мережевому рівнях.

Засоби захисту інформації: *канальний та мережевий рівень* (модуль SIM для зберігання симетричного ключа, який знає лише центр автентифікації вузла зв'язку, ключ використовується при автентифікації та шифруванні кадрів TDMA перед передаванням), *транспортний рівень* (SSL – протокол, що гарантує безпечне передавання даних у мережі, комбінує криптографічну систему з відкритим ключем та блокове шифрування даних, відкритий ключ (RSA) для обміну ключами сесії (RC4 та інші) для групового шифрування, складний протокол управління сесією/зв'язком для встановлення, відновлення, закінчення зв'язку, автентифікація клієнта/сервера через сертифікат X.509), *прикладний рівень* (хешування для генерування MAC, шифрування: RC5; 3DES; Rijndael, цифровий підпис: PKI, RSA, ECDSA, ECC.

Стандарт цифрового безпровідного зв'язку: DECT

Технології захисту інформації: прописування терміналів, автентифікація, удосконалене кодування як захист від прослуховування, скремблювання, шифрування/дешифрування, канальне кодування/ декодування, шумоподібний сигнал з кодовим доступом.

Методи захисту інформації: таємний ключ прописки (PIN), ключі автентифікації та ідентифікації, профілі додатків DECT.

Засоби захисту інформації: шифратори, скремблери.

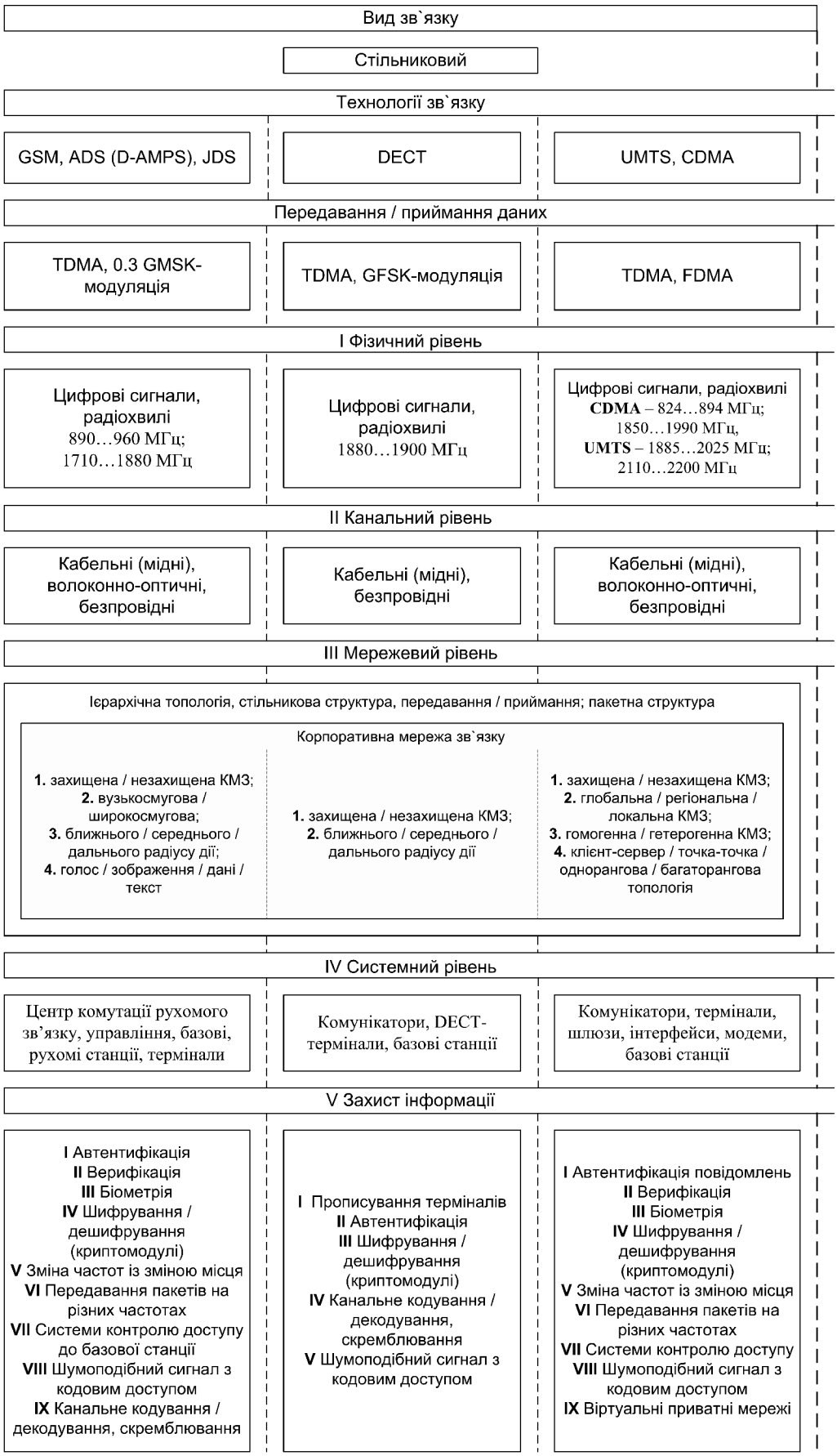

Рис. 2. Концептуальна модель захисту інформації для технологій стільникового зв'язку

Універсальні системи стільникового зв'язку: UMTS, CDMA

Технології захисту інформації: автентифікація повідомлень, верифікація, біометрія, шифрування/дешифрування (криптомодулі), зміна частот із зміною місця, передавання пакетів на різних частотах, системи контролю доступу до базової станції та мережевого обладнання, шумоподібний сигнал з кодовим доступом, віртуальні приватні мережі.

Методи захисту інформації: логін/пароль користувача, стратегія ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи, коди автентифікації, шифрування (RSA) [4], секретність абонента, секретність передавання даних, секретність напрямів з'єднання абонентів, забезпечення цілісності, обмеження доступу до центрального вузла, управління роботою мережі та контроль цієї роботи, забезпечення резервних каналів, забезпечення конфіденційності на канальному та мережевому рівнях [5].

Засоби захисту інформації: *фізичний рівень* (сигнальне скремблювання безпровідного зв'язку, технологія частотного скремблювання радіозв'язку, розширений спектр частот (кожний фрагмент ідентифікується цифровим кодом, який знають термінал отримувача та базова станція), жодний інший термінал не може отримати передавання, для кожного передавання існують мільйони кодових комбінацій), *канальний та мережевий рівень* (забезпечення конфіденційності на канальному та мережевому рівнях, шифрування кожного сегмента дейтаграми перед передаванням, ключ використовується в автентифікації та шифруванні кадрів TDMA перед передаванням), *транспортний рівень* (SSL – протокол, що гарантує безпечне передавання даних у мережі, комбінує криптографічну систему з відкритим ключем та блокове шифрування даних, відкритий ключ (RSA) для обміну ключами сесії (RC4 та інші) для групового шифрування, складний протокол управління сесією/зв'язком для встановлення, відновлення, закінчення зв'язку, автентифікація клієнта/сервера через сертифікат X.509), *прикладний рівень* (автентифікація користувачів, логін/пароль користувача, стратегія ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи, біометрія, цілісність повідомлень, хешування для генерування MAC, шифрування: RC5; 3DES; Rijndael, цифровий підпис: PKI, RSA, ECDSA, ECC [6].

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ТЕХНОЛОГІЙ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Супутникова мережа зв'язку: VSAT

Технології захисту інформації: автентифікація терміналів (апаратний ключ), шифрування/дешифрування (криптомодулі), канальне кодування/декодування, маскування, групування, стискування пакетів даних у протоколах передавання TCP/IP.

Методи захисту інформації: логін/пароль користувача, коди автентифікації, шифрування (RSA)/дешифрування, секретність абонента, секретність передавання даних, секретність напрямів з'єднання абонентів, забезпечення цілісності, управління роботою мережі та контроль цієї роботи, забезпечення резервних каналів, забезпечення конфіденційності на канальному та мережевому рівнях.

Засоби захисту інформації: розширений спектр частот (кожний фрагмент ідентифікується цифровим кодом, який знають термінал отримувача та базова станція), складний протокол управління сесією/зв'язком для встановлення, відновлення, закінчення зв'язку, автентифікація клієнта/сервера через сертифікат X.509, автентифікація користувачів, логін/пароль користувача, стратегія ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи, біометрія, цілісність повідомлень, хешування для генерування MAC, шифрування: RC5; 3DES; Rijndael, цифровий підпис: PKI, RSA, ECDSA, ECC [7–9].

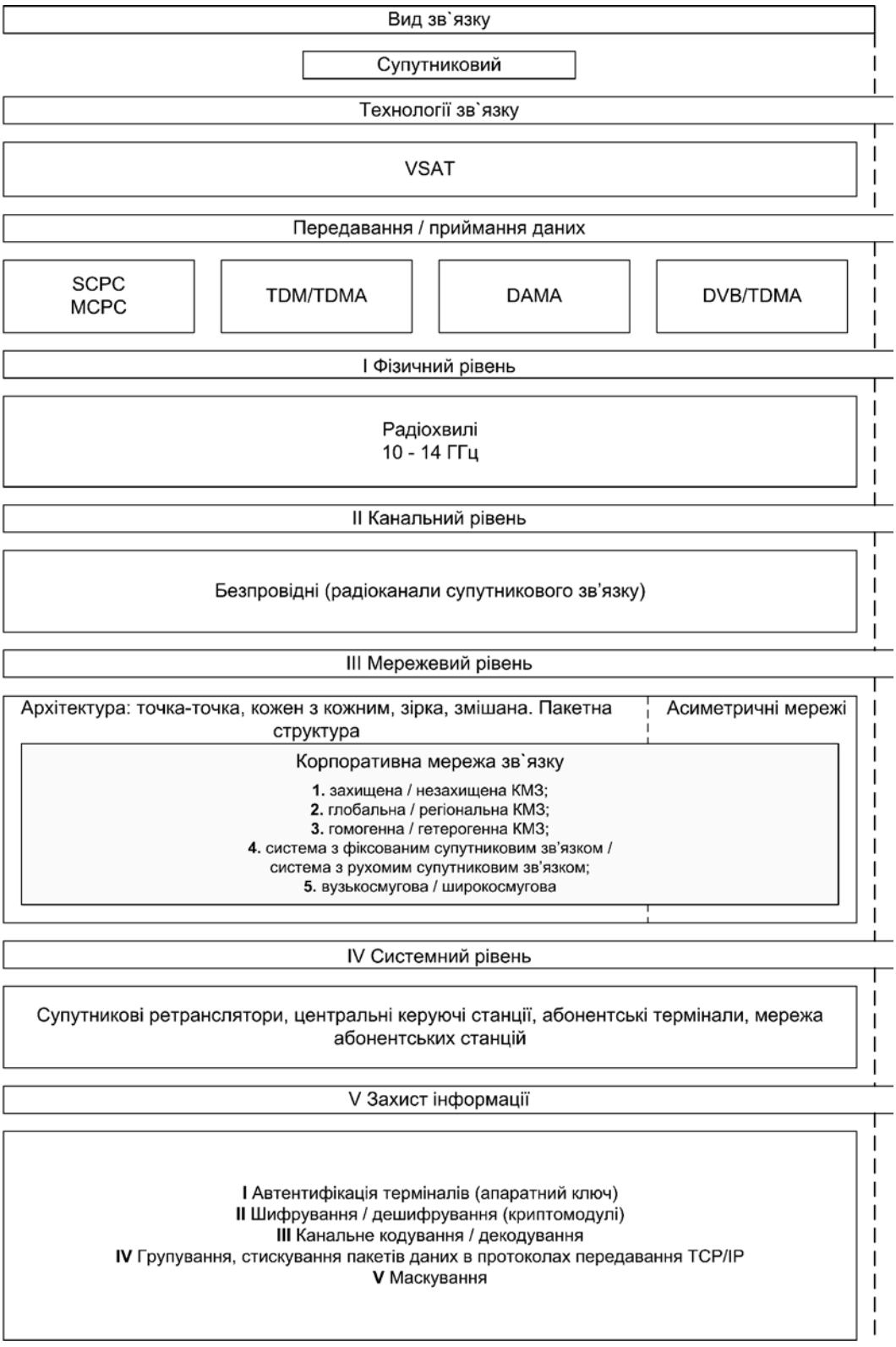

Рис. 3. Концептуальна модель захисту інформації для технологій супутникового зв'язку

Аспекти захисту мовної інформації у корпоративній мережі зв'язку

Корпоративна мережа зв'язку – система каналів зв'язку і під'єднаних до них комп'ютерів, засобів перетворення й розподілу інформації, що забезпечує передавання інформації між різними прикладними програмами, які використовуються в корпорації. Захищена корпоративна мережа – це корпоративна мережа, в якій циркулює інформація з обмеженим доступом, та в якій передбачений її захист від витоку технічними каналами [10].

Досвід експлуатації сучасних корпоративних мереж показує, що проблема інформаційної безпеки вирішується послідовно, здебільшого на вимогу технічних запитів, оскільки наявні технології, методи та засоби не в змозі запобігати порушенням, кількість і різновиди яких зростають щороку.

Вітчизняна специфіка проблеми захисту корпоративних мереж зв'язку [11] полягає в тому, що популярні імпортні засоби, які широко використовуються в нашій державі, не розраховані на застосування у тих ситуаціях, коли безпека має істотне значення, оскільки вони призначені для масового ринку, а не для збирання, оброблення та зберігання конфіденційної інформації. Навантаження додатковими аспектами захисту цих пристроїв, завдяки особливостям їхньої архітектури, не може забезпечити рівень інформаційної безпеки, який вимагають вітчизняні стандарти. Крім того, інформаційна безпека – це галузь, в якій просто неможливо обійтися без вітчизняних розробок та підтримування національних пріоритетів. Відповідно, радикальним виходом у цій ситуації є розроблення вітчизняних захищених систем. Тому актуальним завданням є розроблення загальносистемних принципів та ефективних методів побудови захищених корпоративних мереж зв'язку, впровадження яких сприятиме підвищенню рівня безпеки інформаційних технологій зв'язку.

Різні теоретичні та практичні аспекти проблеми інформаційної безпеки, різні підходи до її вирішення, методи побудови захищених комп'ютерних систем (мереж) досліджуються у великій кількості наукових праць провідних українських та закордонних учених: В.О. Хорошка, В.В. Домарьова, Ю.В. Демченка, П.Д. Зегжди, В.А. Герасименка, С.П. Расторгуєва, Л.М. Ухлінова, А.І. Толстого, С.Н. Смірнова, А.А. Грушо, А.Ю. Щербакова, К. Лендвера, Д. МакЛіна, Р. Сандху, П. Самараті, М. Бішопа, К. Брайса, П. Ньюмена, Т. Джегера.

Функціонування корпоративної мережі зв'язку, рівень її захищеності пов'язані з роботою цифрової системи зв'язку та інформаційної системи (ІС) у її складі. Основним призначенням ІС є програмування роботи ЦСЗ, оброблення та зберігання інформації. Наприклад, у захищеній корпоративній мережі зв'язку існує інформаційна система ProWIN2 (а також FlexGate, Message Systems, FlexCT, FlexAir, Networks Solutions, Flex Encryption, CoralView), яка працює із Program Interface 14. Метою цієї інформаційної системи є програмування цифрової системи зв'язку, якою може бути, наприклад, цифрова система комутації Coral FlexiCom 200.

Захищеність є одним із найголовніших показників ефективності функціонування корпоративної мережі зв'язку поряд із такими показниками, як надійність, відмовостійкість, продуктивність, живучість тощо. Тому покращання цих показників позитивно впливає на функціонування мережі загалом, що і обґрунтовує актуальність та практичну цінність розроблених концептуальних моделей захисту інформації для технологій стаціонарного, стільникового та супутникового зв'язку.

Рівень захищеності КМЗ зумовлений такими аспектами:

– якісний рівень процедури перетворення сигналу (зокрема, мовного) у тракті ЦСЗ;

– якісний рівень оброблення та зберігання сигналів;

– якісний рівень передавання сигналів у каналі (мережі) зв'язку.

До процедури перетворення сигналів в ЦСЗ, зокрема мовних сигналів, належить: у передавальному тракті – форматування (дискретизація, квантування), кодування джерела, шифрування, канальне кодування, імпульсна модуляція, ущільнення; в приймальному тракті – розущільнення, імпульсна демодуляція, канальне декодування, дешифрування, деформатування. Основними методами перетворення мовного сигналу, що запобігають перехопленню і, тим самим, визначають рівень її захищеності, є: накладання захисного шуму; для аналогового каналу – частотні, часові перетворення; для цифрового каналу – перетворення на код з подальшим шифруванням, комбіновані мозаїкові перетворення. Частотні перетворення реалізуються через інверсію спектра, перестановку частотних ділянок (статистичну зміну, керовану криптоблоком). Часові перетворення

реалізуються через: часову інверсію, перестановку відрізків (статистичну зміну, керовану криптоблоком). Перетворення на код реалізуються через: кодування зв'язку (імпульсно-кодову модуляцію або D-модуляцію), кодування голосу (смуговий вокодер).

Ефективність функціонування цієї системи пояснюється її перспективною архітектурою клієнт-сервер, яка передбачає наявність комп'ютерної мережі, розподіленої бази даних, складовими якої є корпоративна база даних та персональні бази даних. Корпоративна база даних розміщується на комп'ютері-сервері.

Відносно розглянутих процедур та методів перетворення сигналів на ефективність функціонування КМЗ, а власне, і рівень захищеності передавальної інформації, зокрема при амплітудно-імпульсній модуляції, впливають параметри: заникання сигналу, кількість каналів, пропускна здатність каналу, відповідно швидкість передавання інформації в каналі (мережі).

Аналіз та розроблення підходів до покращання цих показників, які впливають на рівень захисту інформації, є предметом подальших наукових досліджень.

Висновки

1. Розроблено концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку, які відображають відповідні методи та засоби захисту мовної інформації на рівні фізичних сигналів, каналів, мереж, систем зв'язку.

2. Проаналізовано аспекти захисту інформації у корпоративних мережах зв'язку з урахуванням процедур перетворення інформації в цифровій системі зв'язку та процедур оброблення, зберігання інформації інформаційною системою.

1. Kaufman Charlie. Network Security: Private Communication in a Public World [Text] / Charlie Kaufman, Radia Perlman, Speciner Mike. – Prentice-Hall, 2005. 2. Saadat Malik. Network Security Principles and Practices [Text] / Malik Saadat. – Cisco Press, 2003. 3. Хорошко, В. А. Методы и средства защиты информации [Текст] / В. А. Хорошко, А. А. Чекатков. – Издательство: Юниор, 2003 г. – 504 стр. 4. FIPS PUB 140-2. Security Requirenments for Cryptographic Modules. – U.S. Department of Commerce, NIST, 2001. 5. Stoneburgnen, G. CSPP-OS-COTS Security Protection Profile – Operating Systems. Draft Version 0.4 – U.S. Department of Commerce, NIST, 2005. 6. Ленков, С. В. Методы и средства защиты информации. Том 2. Информационная безопасность [Текст] / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – Арий, 2008. – 344 с. 7. 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. – М.: ИПК "Издательство стандартов", 2002. 8. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – М.: ИПК "Издательство стандартов", 2002. 9. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – М.: ИПК "Издательство стандартов", 2002. 10. Гарасим, Ю. Р. Інформаційна безпека захищених корпоративних мереж зв'язку [Текст] / Ю. Р. Гарасим, В. Б. Дудикевич // Вісник Національного університету "Львівська політехніка" "Автоматика, вимірювання та керування". – Львів, 2009. – № (639). – С. 124–132. 11. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. введ. 1997-01-01. – К.: ДСТСЗІ СБ України.