УДК 004.7

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 2, pp. 137-148

ІНФОРМАЦІЙНА МОДЕЛЬ БЕЗПЕКИ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ

В.Б. Дудикевич[1], В.О. Хорошко[2], Г.В. Микитин[1], Р.І. Банах[1], А.І. Ребець[1]

[1] Національний університет «Львівська політехніка»,
вул. С. Бандери, 12, Львів-13, 79013, Україна,
[2] Національний авіаційний университет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

Запропоновано інформаційну модель захисту даних в технологіях зв'язку GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи "об'єкт - загроза - захист".

Ключові слова: об'єкт захисту, загроза інформаційній безпеці, технологія захисту інформації

Інформаційна модель захисту даних в технологіях зв'язку: GSM, PSTN, VoIP, ADSL, Wi-Fi

Захист даних в інформаційно-телекомунікаційних системах – один з основних сегментів Національної програми інформатизації та Концепції технічного захисту інформації в Україні [1, 2]. Триває розвиток нових методів захисту інформації та удосконалення відомих засобів забезпечення безпеки телекомунікаційних систем. Зокрема, в літературі [3] розглянуто принципи побудови систем зв’язку, стандарти та загрози інформаційній безпеці. В роботі [4] запропоновано методику систематизації та представлення експертних знань про комплексні системи захисту інформації, яка забезпечує оцінювання захищеності інформаційних систем та забезпечення рівнів безпеки. В роботі [5] представлено принципи створення захищених мереж стільникового зв’язку, розглянуто заходи та засоби забезпечення якості передавання інформації.

З метою забезпечення цілісної безпеки структури “система – канал зв’язку– система” розглянемо інформаційну модель захисту даних в технологіях голосової телефонії та передавання даних (рис. 1). Модель створена на основі принципів системного аналізу – ієрархічності, багатоаспектності, цілісності і характеризує безпеку технологій GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи “об’єкт – загроза – захист”. На основі інформаційної моделі формується комплекс уніфікованих методів і засобів забезпечення безпеки даних в технологіях зв’язку відповідно до нормативного забезпечення.

Технологія GSM: характеристика системи “об’єкт – загроза – захист”.

Технологія GSM (Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом TDMA та середнім ступенем безпеки. Технологія GSM відноситься до мереж 2-го покоління (2G – цифровий стільниковий зв'язок), хоча з 2010 р. умовно знаходилась у фазі 2.75G завдяки численним розширенням. Технологія GSM функціонує в чотирьох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц. Загальна архітектура технології GSM представлена на рис. 2.

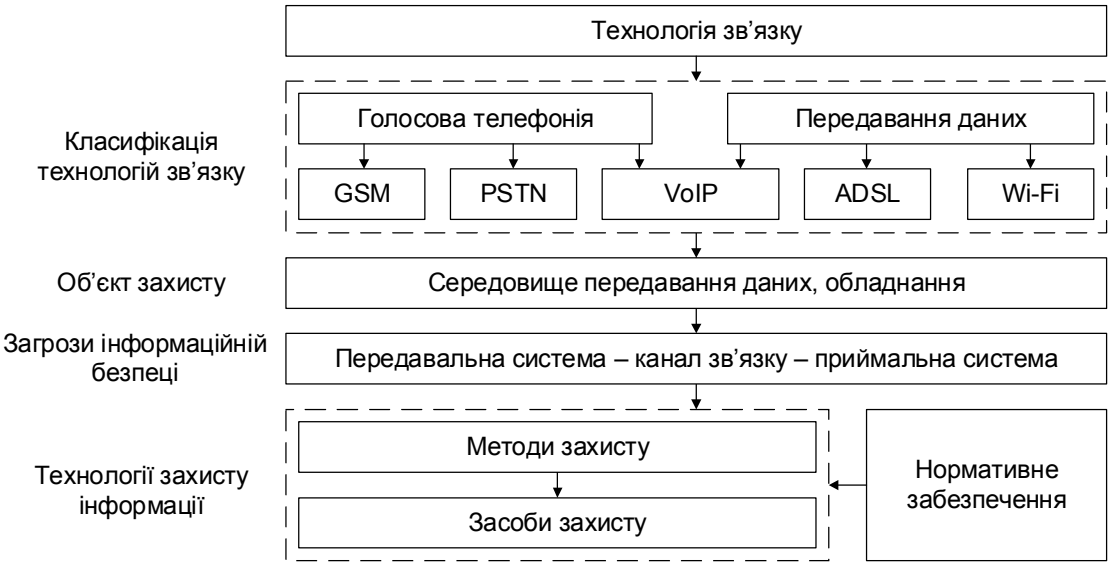

Рис. 1. Інформаційна модель захисту даних в технологіях зв'язку

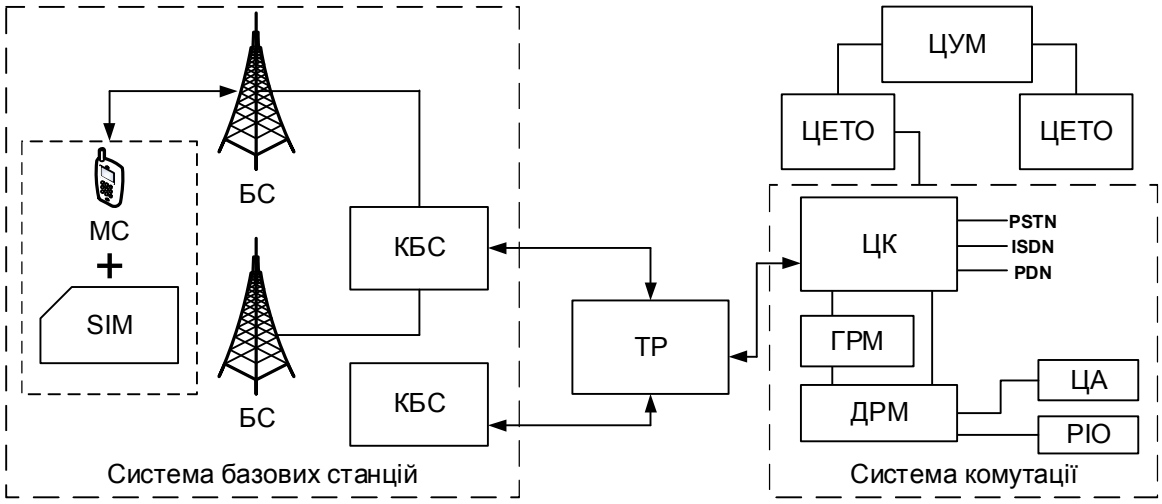

Рис. 2. Загальна архітектура технології GSM

Мобільна станція (МС) із мікропроцесорною картою SIM (Subscriber Identify Modul), в яку занесені унікальні дані для обміну інформацією між абонентами. Контролери базових станцій (КБС) – здійснюють керування базовими станціями (БС) і в подальшому формують з'єднання з центром комутації (ЦК), за допомогою якого можна створити канал передавання даних між двома абонентами. Транскодер (ТР), як проміжна ланка між БС та системою комутації, забезпечує перетворення вихідних сигналів каналу передавання мовного сигналу і даних (64 Кбіт/с) до виду, що відповідає рекомендаціям GSM по радіоінтерфейсу (13 Кбіт/с). В домашньому реєстрі місцезнаходження (ДРМ) зберігається інформація про місцезнаходження будь-якої МС, яка дозволяє центру комутації реалізувати виклик до цієї станції.

Загалом ДРМ представляє базу даних (БД), в якій зберігається службова інформація про абонента. Гостьовий реєстр місцезнаходження (ГРМ) – це тимчасова БД абонентів, які знаходяться в зоні дії відповідного центру комутації. У кожного ЦК є лише один гостьовий реєстр місцезнаходження. В ГРМ зберігається та ж інформація

що і в ДРМ, але лише до того часу допоки МС знаходиться в зоні дії цього ГРМ. Центр автентифікації (ЦА) – це сервіс, за допомогою якого перевіряється право на доступ абонента до мережі, зокрема формуються ключі та алгоритми автентифікації. В ЦА зберігаються: унікальні номери абонента, індивідуальний ключ, алгоритм автентифікації. Реєстр ідентифікації обладнання (РІО) – сервіс, в якому знаходиться централізована БД для підтвердження міжнародного ідентифікаційного номеру МС (IMEI). Центр експлуатації технічного обслуговування (ЦЕТО) – забезпечує контроль і керування іншими компонентами мережі та контроль якості її роботи. Центр управління мережею (ЦУМ) – дозволяє забезпечити раціональне ієрархічне управління мережею GSM та відповідає за експлуатацію і технічне обслуговування.

В GSM використовується дві смуги частот: uplink (трансмісія вгору) 890 – 915 МГц, яка призначена для передавання даних від МС до БС; downlink (трансмісія вниз) 935 – 960 МГц відповідно для передавання інформації від БС до МС. Кожна із смуг дозволяє організувати по 124 симплексних канали із частотним рознесенням між каналами до 200 кГц.

Враховуючи архітектуру, функціонування та особливості технології GSM розглянемо характеристику системи “об’єкт – загроза – захист” згідно інформаційної моделі (рис. 1) (табл. 1) [6, 7, 8].

Технологія PSTN: характеристика системи “об’єкт – загроза – захист”.

Технологія PSTN (Public Switched Telephone Network) – це телефонна мережа загального користування (ТМЗК), для доступу до якої використовуються: проводові телефонні апарати, автоматичні телефонні станції (АТС), обладнання передавання даних. Передавання сигналів, налаштування з’єднання, розмова в технології PSTN реалізуються через універсальну лінію зв'язку від АТС джерела до АТС адресата з особливістю встановлення зв’язку між абонентами за умови розмови двох (рис. 3).

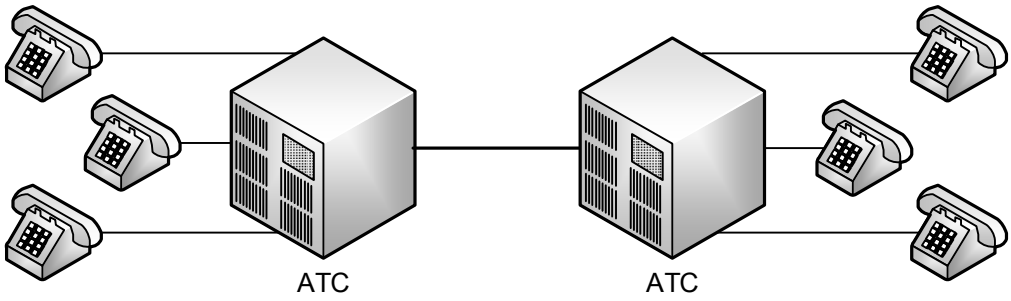

Рис. 3. Загальна архітектура технології PSTN

Технологія PSTN нормативно забезпечена стандартами Міжнародного союзу електрозв'язку (ITU-T) і на практиці здебільшого реалізується за зіркоподібною топологією. Поєднання взаємопов'язаних мереж (стандарт Е.163 для ТМЗК) і єдиний міжнародний телекомунікаційний план нумерації (рекомендація Е.164) дозволяють будь-якому абоненту у глобальному адресному просторі набрати телефонний номер будь-якого іншого абонента. Інформація в мережах такого типу передається зі швидкістю до 33.6 Кб/с.

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології PSTN, враховуючи її особливості (табл. 2) [6, 9].

Таблиця 1.

Технологія GSM та її характеристика

GSM		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Ефір: ▪ Мобільна станція ▪ Базові (передавально-приймальні) станції ▪ Провідне середовище, або ефір: ▪ Контролер базових станцій ▪ Транскодер ▪ Центр комутації ▪ "Домашній" регістр місцезнаходження ▪ "Гостьовий" регістр місцезнаходження ▪ Центр автентифікації ▪ Регістр ідентифікації обладнання ▪ Центр експлуатації і технічного обслуговування ▪ Центр управління мережею
Загрози інформаційній безпеці		▪ Знищення або викривлення логічної структури даних ▪ Несанкціоноване отримання інформації та її модифікація ▪ Зашумлення каналу зв'язку
Захист інформації: технології	Методи	▪ Шифрування даних в радіоканалі ▪ Автентифікація повідомлень ▪ Автентифікація користувача ▪ Перепризначення TMSI ▪ Ідентифікація обладнання
	Засоби	▪ Скремблери ▪ Криптофони ▪ Інвертори спектру ▪ Генератори шуму ▪ Змінювачі голосу ▪ SIM-карти ▪ Шифратори ▪ Алгоритми шифрування (A5/1, A5/2, A5/3) ▪ Ідентифікаційний номер рухомого терміналу (IMEI)

Технологія VoIP: система "об'єкт – загроза – захист"

Технологія VoIP (Voice over IP) – технологія передавання медіа-даних в режимі реального часу за допомогою системи протоколів TCP/IP. В технології VoIP аналоговий мовний сигнал від одного абонента дискретизується (кодується), здійснюється компресія та передавання цифровими каналами зв'язку до іншого абонента, де проводиться зворотна операція – декомпресія, декодування і відтворення аналогового сигналу. У випадку, якщо дзвінок надходить на іншу технологію, наприклад PSTN чи GSM, то сигнал проходить через IP-шлюз, який перетворює цифровий (VoIP) сигнал в аналоговий. Для передавання голосу через IP-мережу відбувається процедура стискання сигналу спеціальною програмою-кодеком. Це здійснюється для збільшення швидкості передавання даних відповідно для підвищення якості зв'язку. Рівень безпеки передавання мовної інформації підвищує процедура шифрування даних. Зв'язок між двома VoIP-терміналами можливий лише за

умови сумісних кодеків. З'єднання двох VoIP-терміналів між собою в мережі забезпечується підтримкою однакового протоколу комутації, наприклад SIP (рис. 4).

Таблиця 2.

Технологія PSTN та її характеристика

PSTN		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Провідне середовище: ▪ Обладнання провайдера – АТС – Комутатори ▪ Пристрої клієнти – Телефонні апарати
Загрози інформаційній безпеці		▪ Застосування закладних пристроїв для перехоплення телефонних повідомлень ▪ Перехоплення акустичних коливань з пристроїв, які володіють "мікрофонним ефектом" ▪ Високочастотне нав'язування ▪ Прослуховування приміщень за допомогою виносних мікрофонів ▪ Перехоплення побічних електромагнітних сигналів випромінювання і наведень
Захист інформації: технології	Методи	▪ Контроль параметрів абонентської телефонної лінії (АТЛ) у робочому стані: – Контроль напруги живлення – Контроль струму короткого замикання – Контроль навантажувальної характеристики – Виявлення сторонніх сигналів ▪ Контроль параметрів знеструмлених АТЛ: – Вимірювання опору шлейфа – Вимірювання омічної асиметрії – Вимірювання параметрів імпедансу АТЛ – Контроль вольт-амперної характеристики – Контроль лісажу-характеристики – Контроль перехідної характеристики ▪ Послаблення корисного сигналу ▪ Фільтрація
	Засоби	▪ Засоби контролю АТЛ: – Сторожові – Пошукові – Універсальні ▪ Засоби закриття мовного сигналу: – Скремблери – - Маскувальники – - Вокодери ▪ Нелінійні атенюатори ▪ Загороджувальні фільтри

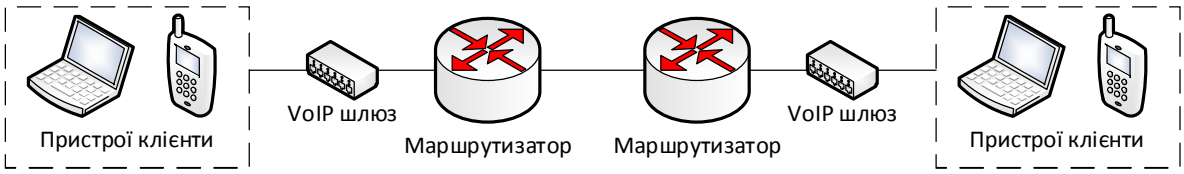

Рис. 4. Загальна архітектура технології VoIP

При передаванні даних в IP-мережах використовуються різні алгоритми стискання мовної інформації, наприклад стискання голосового потоку у 8 і більше разів, а деякі з них практично залишають сигнал на рівні імпульсно-кодової модуляції (64 кбіт/с).

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології VoIP, враховуючи її особливості (табл. 3) [6, 10].

Таблиця 3.

Технологія VoIP та її характеристика

VoIP		Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання		Провідне середовище, або ефір: ▪ Мережеві пристрої – Маршрутизатор – VoIP шлюз ▪ Пристрої клієнти – VoIP телефон / ПК з VoIP програмним забезпеченням
Загрози інформаційній безпеці		▪ Відмова в обслуговуванні (DoS) ▪ Крадіжка реєстраційних даних і маніпуляція ними ▪ Атаки на систему автентифікації ▪ Підміна (спуфінг) Caller ID ▪ Атаки типу "man in the middle" ▪ Атаки типу "Vlan hopping" ▪ Спам через Інтернет-телефонію (SPIT) ▪ VoIP фішинг (Vishing)
Захист інформації: технології	Методи	▪ Ідентифікація/ авторизація користувачів ▪ Перевірка обладнання на право доступу до мережі ▪ Шифрування даних ▪ Забезпечення цілісності ▪ Контроль авторизованих абонентів ▪ Окремий Інтернет-канал для VoIP
	Засоби	▪ Системи виявлення/ запобігання атак ▪ Віртуальні приватні мережі ▪ Брандмауер VoIP ▪ Захищені мережеві протоколи ▪ Міжмережеві екрани ▪ Системи контролю цілісності

Технологія ADSL: система “об’єкт – загроза – захист”

Технологія ADSL (Asymmetric Digital Subscriber Line) – технологія широкосмугового доступу, яка забезпечує передавання швидкісного цифрового сигналу звичайною аналоговою телефонною лінією за умови одночасного користування телефоном та Інтернетом. Технологія ADSL відноситься до класу широкосмугових (broadband) та передбачає організацію асиметричного обміну даними (рис. 5).

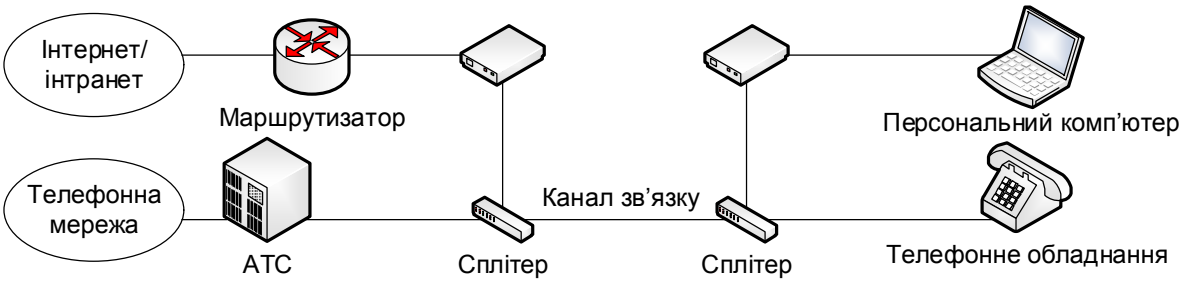

Рис. 5. Загальна архітектура технології ADSL

Технологія забезпечує швидкість передавання даних в напрямку абонента – 24 Мбіт/с, від абонента – 3.5 Мбіт/с. В ADSL мовний сигнал передається в частотному діапазоні 0.3 – 3.4 кГц, а інформація в діапазоні 26 кГц – 1104 МГц, який розділений на два піддіапазони: 26 – 138 кГц (для вихідного потоку даних); 138кГц – 1.1МГц (для вхідного). Особливістю технології ADSL є можливість одночасно працювати в Інтернет і розмовляти телефоном.

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології ADSL, враховуючи її особливості (табл. 4) [11].

Технологія Wi-Fi: система “об’єкт – загроза – захист”

Технологія WI-FI (Wireless Fidelity) – технологія об'єднує декілька протоколів і ґрунтується на системі стандартів IEEE 802.11. На практиці широко використовується протокол IEEE 802.11n, який визначає принцип функціонування безпровідних мереж (рис. 6).

Рис. 6. Загальна архітектура технології Wi-Fi

Таблиця 4.

Технологія ADSL та її характеристика

ADSL		Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних: обладнання		Провідне середовище: ▪ Мережеві пристрої – ADSL модеми – Сплітери ▪ Пристрої клієнти
Загрози інформаційній безпеці		▪ Відмова в обслуговування (DoS) ▪ Крадіжка реєстраційних даних і маніпуляція ними ▪ Атаки на систему автентифікації ▪ Атаки типу "man in the middle" ▪ Несанкціонована модифікація лінії зв'язку
Захист інформації: технології	Методи	▪ Ідентифікація ▪ Автентифікація ▪ Перевірка обладнання на право доступу до мережі ▪ Послаблення корисного сигналу ▪ Фільтрація
	Засоби	▪ Системи ідентифікації/ автентифікації користувачів ▪ Системи виявлення/ запобігання атак ▪ Віртуальні приватні мережі ▪ Брандмауери; ▪ Системи контролю цілісності ▪ Нелінійні атенюатори ▪ Загороджувальні фільтри

Функціонування технології Wi-Fi полягає у підключенні мобільного пристрою до точки доступу, роль якої може виконувати як окремий пристрій, так і мобільний, при правильному налаштуванні. Точка доступу розповсюджує свій ідентифікатор (SSID) в ефір за допомогою спеціальних сигналів (“маячків”).

На сьогодні в Україні функціонують стандарти: IEEE 802.11a (діапазон частот 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11b (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 11 Мбіт/с), IEEE 802.11g (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11n (діапазон частот 2.4 – 2.5 ГГц та 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 320 Мбіт/с); впроваджується IEEE 802.11ac (максимальна швидкість передавання інформації більше 1Гбіт/с).

На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології Wi-Fi, враховуючи її особливості (табл. 5) [12, 13, 14].

Таблиця 5.

Технологія Wi-Fi та її характеристика

Wi-Fi		Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання		Ефір: ▪ Базова станція – Маршрутизатор / безпровідна точка доступу ▪ Клієнтські пристрої – Мобільний пристрій з модулем Wi-Fi
Загрози інформаційній безпеці		▪ Відмова в обслуговування (DoS) ▪ Крадіжка реєстраційних даних і маніпуляція ними ▪ Атаки на систему автентифікації ▪ Спуфінг ▪ Атаки типу "man in the middle" ▪ Несанкціоноване отримання інформації та її модифікація.
Захист інформації: технології	Методи	▪ Ідентифікація/авторизація користувачів ▪ Перевірка обладнання на право доступу до мережі ▪ Приховування ідентифікатора мережі ▪ Шифрування даних ▪ Забезпечення цілісності ▪ Обмеження доступу до центрального вузла ▪ Контроль авторизованих абонентів
	Засоби	▪ Брандмауери ▪ Базові системи автентифікації ▪ Протоколи шифрування ▪ Модель AAA (Authentication Authorization Accounting) ▪ Системи виявлення/запобігання атак ▪ Системи приманки ▪ Системи контролю цілісності

Нормативне забезпечення системи “об’єкт – загроза – захист” для технологій зв’язку

На основі інформаційної моделі захисту мовної інформації в ІКТ (рис. 1) розглянемо елементи нормативного забезпечення системи “об’єкт – загроза – захист”, що є основою застосування уніфікованих методів і засобів забезпечення безпеки передавання даних в тракті “система – канал зв’язку – система” (табл. 6).

Таблиця 6.

Нормативне забезпечення захисту мовної інформації в ІКТ

Закони та постанови	▪ Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 №80/94-ВР ▪ Постанова Кабінету міністрів “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 29.03.2006 № 373. Остання редакція від 13.10.2011.
Стандарти	1. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1997-01-01] – К.: Держстандарт України, 1996 – 20 с. – (Державний стандарт України).

Продовження таблиці 6.

	2. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – [Чинний від 1997-07-01] – К.: Держстандарт України, 1996 – 4с. – (Державний стандарт України). 3. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 1998-01-01] – К.: Держстандарт України, 1997 – 6 с. – (Державний стандарт України). 4. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145-2002. – [Чинний від 2003-07-01]. – К.: Держспоживстандарт України, 2002. – 38 с. – (Національний стандарт України). 5. Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO/IEC 10118 – 1 : 2000, IDT): ДСТУ ISO/IEC 10118-1:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 10 с. – (Національний стандарт України). 6. Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використанням n-бітового блокового шифру (ISO/IEC 10118 – 2 : 2000, IDT): ДСТУ ISO/IEC 10118-2:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 24 с. – (Національний стандарт України). 7. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC 14888-1:1998, IDT): ДСТУ ISO/IEC 14888-1-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 18 с. – (Національний стандарт України). 8. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів (ISO/IEC 14888 – 2 : 1999, ГОТ): ДСТУ ISO/IEC 14888-2-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 22 с. – (Національний стандарт України). 9. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів (ISO/IEC 14888 – 3 : 1998, IDT): ДСТУ ISO/IEC 14888-3-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 34 с. – (Національний стандарт України). 10. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: ГОСТ Р ИСО/МЭК 13335-1-2006. – [Чинний від 2007-06-01]. – М.: Стандартинформ, 2007. – 23 с. – (Межгосударственный стандарт). 11. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-001-99. – [чинний від 1999-07-01]. – К.: ДСТСЗІ СБ України, 1999 – 56 с. – (Нормативний документ).

Продовження таблиці 6.

	12. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-002-99. – [чинний від 1999-07-01]. – К.: ДСТСЗІ СБ України, 1999 – 16 с. – (Нормативний документ). 13. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 06.04.2001 №11: НД ТЗІ 2.3-002-2001 [чинний від 2001-04-10]. – К.: ДСТСЗІ СБ України, 2001 – 11 с. – (Нормативний документ). 14. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. – [Чинний від 2005-11-08]. – К.: ДСТСЗІ СБ України, 2005. – 16 с. – (Нормативний документ системи технічного захисту інформації). 15. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 49 с. – (Галузевий стандарт України). 16. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 163 с. – (Галузевий стандарт України).

Висновок

Запропонована інформаційна модель захисту даних в технологіях зв'язку дозволяє забезпечити цілісну безпеку на рівні системи "об'єкт – загроза – захист" для передавально-приймального тракту "система – канал зв'язку – система", що є методологічною основою для застосування уніфікованих методів і засобів захисту інформації згідно діючих стандартів у сфері інформаційно-комунікаційних технологій.

Список літератури

1. Закон України "Про Національну програму інформатизації" від 4 лютого 1998 року №74/98-ВР. Остання редакція від 02.12.2012. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
2. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 № 1126. Остання редакція від 13.10.2011. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1126-97-%D0%BF,415.
3. Щербаков, В. Б. Защита беспроводных телекоммуникационных систем: учеб. пособие / В. Б. Щербаков, А. В. Гармонов, С. А. Ермаков и др. – Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. – 127 с.
4. Рибачек, Н. І. Аналіз захищеності інформаційної системи / Н. І. Рибачек // К.: Національний технічний університет України "Київський політехнічний інститут": Прикладна математика та комп'ютинг, 2010. – С. 122-125.

5. Kargl, F. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges / F. Kargl, P. Papadimitratos, L. Buttyan and other // IEEE Communications Magazine. – November, 2008. – P. 110-118.
6. Дудикевич, В. Б. Захист засобів і каналів телефонного зв'язку: Навчальний посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Л.: Видавництво Львівської політехніки, 2012. – 210 с.
7. Попов, В. И. Основы сотовой связи стандарта GSM / В. И. Попов. – М.: Эко-Трендз, 2005. – 296 с.
8. GSM Overview. Telecomspace. – [Електронний ресурс]. – Режим доступу: http://www.telecomspace.com/ gsm.html.
9. Дудикевич, В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету "Львівська політехніка": Автоматика, вимірювання та керування, 2010. – № 665. – С. 18-26.
10. Вайнгартнер, М. Защита голосовых соединений VoIP от прослушивания / М. Вайнгартнер // Журнал сетевых решений/LAN, 2003. – № 12. – [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/2003/12/138398.
11. Челнокова, О. ADSL-маршрутизаторы с поддержкой VPN / О. Челнокова // Information Security / Информационная безопасность, 2008. – №2. – С. 32-33.
12. Ramachandran, V. BackTrack 5 Wireless Penetration Testing Beginner's Guide / V. Ramachandran. – Birmingham: Packt Publishing Ltd., September 2011. – 207 p.
13. Владимиров, А. А. Wi-фу: "боевые" приемы взлома и защиты беспроводных сетей. Серия "Защита и администрирование" / А. А. Владимиров, К. В. Гавриленко, А. А. Михайловский. – М.: NT Press, 2005. – 463 с.
14. Гордейчик, С. В. Безопасность безпроводных сетей / С. В. Гордейчик, В. В. Дубровин. – М.: Горячая линия - Телеком, 2008. – 288 с.

ИНФОРМАЦИОННАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ СВЯЗИ

В.Б. Дудикевич[1], В.А. Хорошко[2], Г.В. Микитин[1], Р.И. Банах[1], А.И. Ребець[1]

[1] Национальный авиационный университет,
пр. Космонавта Комарова, 1, Киев, 03058, Украина;
[2] Национальный университет «Львовская политехника»,
ул. С. Бандеры, 12, Львов 13, 79013, Украина, e-mail: professor_va@ukr.net

Предложена информационная модель безопасности данных в технологиях связи GSM, PSTN, VoIP, ADSL, Wi-Fi на уровне системы "объект - угроза - защита".
Ключевые слова: объект защиты, угроза информационной безопасности, технология защиты информации

INFORMATION SECURITY MODEL FOR COMMUNICATION TECHNOLOGIES

V.B. Dudikevich[1], V.O. Khoroshko[2], G.V. Mikitin[1], R.I. Banach[1], A.I. Rebets[1]

[1] National University «Lviv Polytechnika»,
12 S.Bandera str., Lviv -13 , 79013, Ukraine
[2] National Aviation University,
1, prosp. Kosmonavta Komarova, Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net

Information model for data security in GSM, PSTN, VoIP, ADSL, and Wi-Fi communication technologies at the level of "asset-threat-protection" system was proposed.
Keywords: asset to be protected, information security threat, information security technology.