УДК 004.07

В.Б. Дудикевич,
Г.В. Микитин,
А.І. Ребець,
Р.І. Банах

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ

Запропоновано комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку GSM, CDMA, WiMAX, LTE на основі принципів системного аналізу, який дозволяє формувати структури безпеки даних в системі, каналі, передавально-приймальному тракті згідно з концепцією "об'єкт – загроза – захист".

Ключові слова: *технології зв'язку, мовна інформація, захист, комплексний підхід.*

Предложен комплексный подход к защите речевой информации в технологиях беспроводной связи GSM, CDMA, WiMAX, LTE на основе принципов системного анализа, который позволяет формировать структуры безопасности данных в системе, канале, приемо-передающем тракте согласно концепции "объект – угроза – защита".

Ключевые слова: *технологии связи, речевая информация, защита, комплексный подход.*

A complex approach was proposed to secure speech information in wireless technologies GSM, CDMA, WiMAX, LTE on the basis of system analysis principles. Such an analysis allows to form the structure of data security in a system, a channel, a transfer-recipient path according to the concept 'object – threat – defense'.

Keywords: *wireless technologies, speech information, security, complex approach.*

1. Структура комплексного підходу до захисту мовної інформації в технологіях безпровідного зв'язку

Безпека інформаційно-комунікаційних технологій (ІКТ) є одним з основних завдань Національної програми інформатизації України та входить до основних розділів Концепції технічного захисту інформації [1, 2]. Технічний захист інформації в міжнародних телекомунікаційних системах є основним сегментом системи забезпечення інформаційної безпеки держави на рівні напрямів взаємодії в єдиному інформаційному просторі [3]. У контексті забезпечення конфіденційності, цілісності та доступності інформації актуальними залишаються аспекти захисту мовного сигналу (МС) в безпровідних інформаційно-комунікаційних технологіях [4].

Питання розроблення методів і засобів захисту мовної інформації в безпровідних ІКТ висвітлені в роботах [5, 6, 7, 8, 9, 10].

Метою роботи є забезпечення цілісної інформаційної безпеки на основі створення комплексного підходу до захисту даних в технологіях безпровідного

зв'язку, який враховує імовірні загрози системного, сигнального, канального рівнів і тракту "система – канал – система" в цілому. Розглянемо особливості функціонування деяких технологій безпровідного зв'язку.

Технології зв'язку: GSM, CDMA, WiMAX, LTE. Інформаційно-комунікаційна технологія – це інформаційні процеси і методи роботи з інформацією, які здійснюються із застосуванням засобів обчислювальної техніки і засобів телекомунікації [11].

Технологія *GSM (Global System for Mobile communication)* – міжнародний стандарт для цифрового безпровідного зв'язку другого покоління з часовим та частотним розділенням каналів і середнім рівнем безпеки, розроблений Європейським інститутом стандартизації електрозв'язку (*ETSI*).

Мережі *GSM* функціонують на основі використання великої кількості базових станцій (БС), які розгорнуті на місцевості і частково перекриваються. При вхідному/ вихідному виклику мобільний телефон з'єднується з найближчою БС і сигнал передається на керуючий блок станції, який здійснює розподіл ресурсів між абонентами. Декілька БС, які обслуговують відповідну територію, під'єднані до контролера локальної зони. Контролери комутуються з центром керування мобільними послугами, який забезпечує контроль викликів, а також вхід / вихід на місцеві телефонні лінії та інших операторів безпровідного зв'язку [12].

Технологія *CDMA (Code Division Multiple Access)* – одна з технологій множинного доступу з кодовим розділенням каналів. Принцип функціонування *CDMA*: кожному джерелу інформації виділяється індивідуальний код, за допомогою якого кодується вихідне повідомлення. Приймач за відомим кодом виділяє закодоване повідомлення потрібного відправника з потоку інших повідомлень. В мережах безпровідного зв'язку 2-го та 3-го покоління, зокрема в стандарті *CDMA 2000*, технологія множинного доступу використовується на ділянці між БС та мобільним обладнанням [13].

Технологія *WiMAX* (*Worldwide Interoperability for Microwave Access*) – стандарт, що забезпечує широкосмуговий безпровідний зв'язок між абонентами на великі відстані.

Мережа *WiMAX* побудована на основі базових і абонентських станцій та обладнання, яке зв'язує між собою БС та Інтернет-провайдера. Між БС встановлюється з'єднання у частотному діапазоні 10–66 ГГц – прямої видимості. Між БС та абонентами встановлюється з'єднання у частотному діапазоні 1,5–11 ГГц – без прямої видимості [14]. В літературі [15] представлені особливості архітектури мережі *WiMAX* у контексті взаємодії з мережами безпровідного зв'язку різних стандартів та аспекти її розвитку.

Технологія *LTE* (*Long Term Evolution*) – мобільний стандарт високошвидкісного передавання даних четвертого покоління, що базується на мережевих технологіях *GSM/EDGE (Enhanced Data Rates for GSM Evolution)* та *UMTS (Universal Mobile Telecommunications System) / HSPA (High Speed Packet Access)*.

Мережа *LTE* складається з двох основних елементів: мережі радіодоступу *E-UTRAN (Evolved Universal Terrestrial Access Network)* і базової мережі *SAE (System Architecture Evolution)*. *E-UTRAN* складається з базових станцій *eNB (Evolved Node B)*, які з'єднані між собою та з базовою мережею, побудованою за принципом комутації пакетів. *SAE* містить вузли *MME (Mobility Management Entity)* та *UPE (User Plane Entity)*, які відповідають за вирішення завдань керування

мобільністю абонентського терміналу та передачу даних користувача відповідно [16, 17].

Актуальними є принципи побудови та функціонування мереж *LTE*, спектр загроз інформаційній безпеці, а також методи і засоби захисту даних [9, 18].

Структура комплексного підходу до захисту мовного сигналу. З метою забезпечення безпечного функціонування технологій безпровідного зв'язку пропонується комплексний підхід до захисту МС на основі концепції "об'єкт – загроза – захист" (рис. 1) [19].

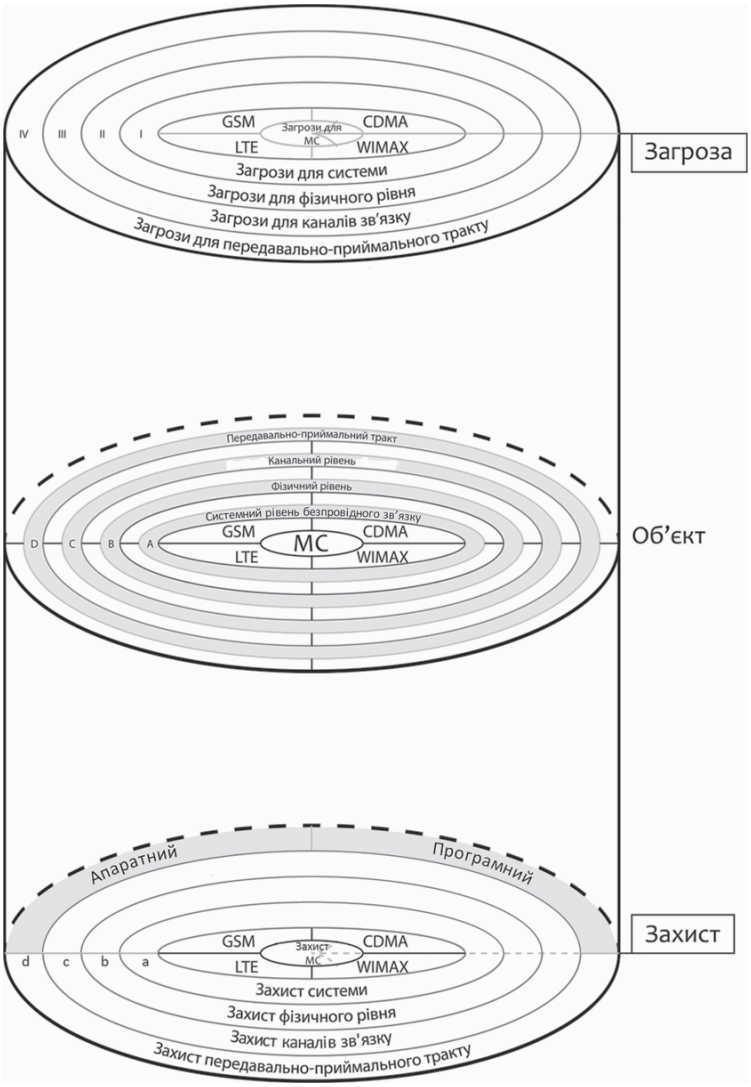

Рис. 1. Структура комплексного підходу до захисту мовного сигналу в технологіях зв'язку: *GSM, CDMA, WIMAX, LTE*

Центральним сегментом структури підходу (A–B–C–D) є елементи технологій зв'язку ***GSM, CDMA, WiMAX, LTE*** – системи, сигнали, канали, передавально-приймальні тракти. Верхній сегмент підходу (I–II–III–IV) являє загрози для системного, фізичного, канального рівнів і передавально-приймального тракту. У нижньому сегменті розташовано елементи апаратного і програмного захисту відповідно до систем, сигналів, каналів, передавально-приймальних трактів.

2. Концепція "об'єкт – загроза – захист" в технологіях зв'язку

Модель об'єкта захисту. Розглянемо елементи захисту МС в технологіях зв'язку *GSM, CDMA, WiMAX, LTE* на рівнях: системному (A), фізичному (B), канальному (C), передавально-приймального тракту (D).

Рівень A. Технології безпровідного зв'язку на системному рівні передавання / приймання радіосигналів у відповідних частотних діапазонах відрізняються одна від одної відповідним обладнанням. Зокрема, для *GSM* – це центр комутації рухомого зв'язку, центр автентифікації абонентів, управління, базові, рухомі станції, термінали, шлюзи; для *CDMA* – центр комутації рухомого зв'язку, центр управління і обслуговування, базові, рухомі станції, комунікатори, термінали, шлюзи, інтерфейси, модеми; для *WiMAX* – модеми, мобільні пристрої, базові та абонентські станції; для *LTE* – вузол керування мобільністю, базові станції, модеми, термінали, шлюзи. На системному рівні безпеки технологій безпровідного зв'язку актуальним залишається розвиток апаратно-програмного забезпечення захисту мовного сигналу [12, 18, 20].

Рівень B. Об'єктом захисту технологій на фізичному рівні є радіосигнали, які передаються з мобільних терміналів та стаціонарних базових станцій. Частотні діапазони радіосигналів для технологій зв'язку представлені в таблиці 1.

Таблиця 1

Радіосигнали в технологіях безпровідного зв'язку

Технологія зв'язку	Частотний діапазон
GSM	890–960; 1710–1880 МГц
CDMA	824–849; 869–894 МГц; 1920–1980; 2110–2170 МГц
WiMAX	до абонента: 1,5–11 ГГц; між станціями: 10–66 ГГц
LTE	для частотної модуляції: 700–2700 МГц; для часової модуляції: 1800–3800 МГц

Рівень C. Елементом захисту мовного сигналу в технологіях безпровідного зв'язку є канальний рівень. Для технологій *GSM, CDMA*, *WiMAX* та *LTE* використовують безпровідні та провідні канали зв'язку, що характеризуються амплітудно-частотною характеристикою та пропускною здатністю.

Рівень D. У контексті захисту МС на рівні передавально-приймального *тракту* передбачені процедури перетворення: форматування / деформатування, шифрування / дешифрування, канальне кодування / декодування, імпульсна модуляція / демодуляція, ущільнення / розширення т. і.

Модель загроз для технологій зв'язку. Згідно з комплексним підходом до захисту мовної інформації модель загроз для технологій зв'язку представлена на рівні: системи (I); фізичного сигналу (II); каналу зв'язку (III); передавально-приймального тракту (IV).

Рівень I. Для складових систем безпровідного зв'язку характерні такі загрози перехоплення мовної інформації: прослуховування мобільних телефонів; стороннє підключення пристроїв зчитування інформації до комунікаторів; несанкціонований віддалений доступ до терміналів і шлюзів; фізичний доступ до базових станцій

та мобільних терміналів та ін. [21]. Загрозами системного рівня є: помилки при адмініструванні систем, неправильна установка, конфігурування; підміна довіреного об'єкта; несанкціоноване переконфігурування радіоапаратури; DoS (DDos) ((Distributed) Denial-of-service attack) атаки [9].

Рівень II. Для фізичного рівня технологій безпровідного зв'язку – сигналів, характерні, зокрема, такі загрози: пошкодження передавання даних у відповідних частотних діапазонах радіосигналу; перехоплення (прослуховування) ефіру; модифікація даних у трафіку [22].

Можливе створення завад для приглушення частотного діапазону з метою унеможливлення здійснення виклику за допомогою безпровідної системи зв'язку. Така дія може бути ненавмисною – за недостатньої захищеності базових станцій для передачі радіосигналу і цілеспрямованою – при використанні пристроїв для приглушення радіосигналу.

Актуальними залишаються загрози перехоплення і розшифрування GSM-сигналів. Прилади для прослуховування сигналів GSM-зв'язку (наприклад, апаратно-програмний комплекс PostWin, система моніторингу GSM Interceptor Pro т. і.) здійснюють: контроль каналу базової станції; контроль каналу мобільного телефону; сканування усіх каналів і пошук активних (у певній точці); запис сигналу (мовної інформації) на носії даних; реєстрацію номерів абонента, який викликається [23].

Рівень III. Канал зв'язку (зокрема, локальна мережа) – складова безпечного передавання/ приймання даних. Серед загроз канального рівня, які найбільше проявляються на практиці: вплив сторонніх сигналів, сформованих передавачами, що працюють на частоті інформаційного сигналу; вплив комплексу зовнішніх факторів на параметри мовного сигналу [24].

Рівень IV. Загрозами для передавально-приймального тракту "система – канал – система" є побічні електромагнітні випромінювання та наведення у контексті перехоплення інформації, а також прилади високої напруги як засоби впливу на корисний сигнал. Вплив цих та інших факторів може призвести до пошкодження підсилювачів радіочастотного діапазону, виведення з ладу базової станції. Відповідно, МС втрачає інформативність, знижується достовірність його приймання [25].

Модель захисту технологій зв'язку. Модель захисту технологій безпровідного зв'язку представлена на рівні: системи (a), сигналу (b), каналу (c), передавально-приймального тракту (d) (рис. 1).

Рівень a. Захист системи від перехоплення МС передбачає: вибір телефонів, які перевірені на відсутність пристроїв прослуховування; зменшення ймовірності доступу зловмисника до системи (насамперед уникнення передавання конфіденційної інформації стільниковим телефоном); врахування аспектів складності перехоплення МС з рухомого об'єкта; використання систем зв'язку, в яких дані передаються з великою швидкістю за багатократної автоматичної зміни частот упродовж розмови [26]. Для терміналів доцільно обмежити фізичний доступ до системи кодовим чи ключовим замком. При програмному віддаленому доступі необхідно використовувати складні паролі, довжина яких більша за 8 символів.

Рівень b. Захист технологій зв'язку на фізичному рівні відбувається за допомогою вбудованих алгоритмів шифрування, зокрема: для *GSM*: A5/1, A5/2, A5/3; *CDMA*: CAVE; *WiMAX*: DES3, AES; *LTE*: AES, AKA [27, 28].

Розглянемо алгоритми шифрування, які використовуються в технології *WIMAX*. Алгоритм *DES3* (*Triple DES, 3DES*) – симетричний блоковий шифр, створений на основі алгоритму DES (*Data Encryption Standard*). Швидкість роботи 3DES в 3 рази нижча, ніж у DES, але криптостійкість є вищою. Сьогодні алгоритм DES не забезпечує усіх критеріїв захисту МС, тому для шифрування даних ефективно використовується алгоритм AES як доповнення до стандарту IEEE 802.16e. Алгоритм *AES* (*Advanced Encryption Standard*) – метод шифрування, який ґрунтується на використанні симетричного ключа і є однією з криптосистем, яку використовують у *3GPP (3rd Generation Partnership Project)*. Стандарт 802.16e визначає використання шифрування AES в чотирьох режимах: зчеплення блоку шифрів, шифрування лічильника, шифрування лічильника із кодом аутентифікації зчепленням блоку шифрів, електронної кодової книги

Рівень c. Одним з ефективних методів захисту мовної інформації у технологіях безпровідного зв'язку є модуляція сигналу з частотним і часовим ущільненням, зокрема, в: *GSM* – TDMA (множинний доступ з розділенням каналів по часу), GMSK (Гаусівська маніпуляція із мінімальним зсувом частоти); *CDMA* – TDMA, FDMA (множинний доступ з розділенням каналів відповідно по часу і частоті); *WIMAX* – FDD (частотний дуплексний розподіл), TDD (часовий дуплексний розподіл), OFDM (ортогональне ущільнення із частотним розподілом); *LTE* – FDD (OFDM, SC-FDMA (частотне розділення одного підканалу з множинним доступом)), TDD [24, 29].

Рівень d. Модель безпеки технологій зв'язку на рівні передавально-приймального тракту – синтез методів і засобів захисту МС на апаратно-програмному рівнях.

Апаратний захист МС в технологіях безпровідного зв'язку забезпечує конфіденційність мовної інформації в тракті, зокрема на рівні скремблювання та зашумлення [30, 31].

Програмний захист даних в передавально-приймальному тракті технологій зв'язку передбачає створення програмного забезпечення засобів безпеки мовної інформації, зокрема на рівні алгоритмів шифрування [32].

Розроблено комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку на основі концепції "об'єкт – загроза – захист". Розглянуто елементи апаратного і програмного забезпечення захисту даних на рівні: системи, каналу, передавально-приймального тракту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну програму інформатизації : Закон України від 4 лютого 1998 року №74/98-ВР. [Електронний ресурс]. – Режим доступу : http : // zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

2. Про затвердження Концепції технічного захисту інформації в Україні : Концепція технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.1997 № 1126 [Електронний ресурс]. – Режим доступу : http : // zakon4.rada.gov.ua/laws/show/1126-97-%D0%BF,415.

3. Доктрина інформаційної безпеки України. Указ Президента України від 08.07.2009 № 514/2009 // Офіційний вісник України. – 2009. – № 52. – С. 7 [Електронний ресурс]. – Режим доступу : http : // zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009.

4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу : http : // zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

5. *Гольдштейн Б.С.* Сети связи / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб: БХВ-Петербург, 2010. – 400 с.

6. Система анализа данных и обнаружения изменения уровня безопасности передачи данных в беспроводных сетях / Д.М. Михайлов, А.В. Стариковский, А.В. Зуйков, А.М. Толстая // Журнал "Спецтехника и связь". – 2013. – № 5. – С. 23–30.

7. *Колыбельников А.И.* Обзор технологий беспроводных сетей / А.И. Колыбельников // Труды МФТИ. – 2012. – Т. 4. – № 2. – С. 3–29.

8. *Місюра С.М.* Варіант захисту мовної інформації на об'єктах інформаційної діяльності / С.М. Місюра В.В. Овсяннiков, І.Р. Мальцева // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2011. – № 2. – С. 84–93.

9. 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.

10. *Семенко А.І.* Сучасний стан створення безпровідних телекомунікаційних систем / А.І. Семенко // Вісн. Нац. ун-ту "Львів. Політехніка". Радіоелектрон. та телекомунікації. – 2009. – № 645. – С. 56–67.

11. Информационно-коммуникационные технологии в образовании. Термины и определения : ГОСТ Р 52653–2006. – Действующий от 2006-12-27. – М. : Стандартинформ, 2007. – 11 с. – (Национальный стандарт Российской Федерации).

12. Как устроена сеть сотовой связи GSM/UMTS. Портал "Хабрахабр" [Электронный ресурс]. – Режим доступа : http : // habrahabr.ru/post/82757/.

13. CDMA (Code Division Multiple Access). Сотовая связь : история, стандарты, технологии [Электронный ресурс]. – Режим доступа : http : // celnet.ru/CDMA.php.

14. *K. Etemad* WiMAX Technology and Network Evolution / K. Etemad, M.-Y. Lai. – New York City : Wiley-IEEE Press, 2010. – 408 p.

15. *Вишневский В.* Энциклопедия WiMAX. Путь к 4G / В. Вишневский, С. Портной, И. Шахнович. – М. : Техносфера, 2009. – 472 с.

16. *Тихвинский В.О.* Сети мобильной связи LTE. Технологии и архитектура / В.О. Тихвинский, С.В. Терентьев, А.Б. Юрчук. – М. : Эко-Трендз, 2010. – 284 с.

17. LTE : взгляд изнутри. Портал "Хабрахабр" [Электронный ресурс]. – Режим доступа : http ://habrahabr.ru/post/136317/.

18. *Гельгор А.Л.* Технология LTE мобильной передачи данных : учеб. пособие / А.Л. Гельгор, Е.А. Попов. – СПб. : Изд-во политехн. ун-та, 2011. – 204 с.

19. 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).

20. Сотовые сети стандарта CDMA. – [Электронный ресурс]. – Режим доступа : http : // kunegin.narod.ru/ref3/mob/8.htm .

21. *Скребнев В.* Системы безопасности и видеонаблюдения / В. Скребнев [Электронный ресурс]. – Режим доступа : http : // www.bughunter.ru/stat/stat_09.php.

22. *Wilson P.* Vulnerability of Wireline and Cellular Telecommunications Networks to High Power Radio Frequency Fields / P. Wilson. – Darby : DIANE Publishing, 2009. – 30 p.

23. Оборудование мониторинга для специальных служб. Intercept Monitoring Systems [Электронный ресурс]. – Режим доступа : http : // www.intercept.ws/.

24. Оцінка якості відновлення мови в захищених безпроводових каналах зв'язку / Г.Ф. Коханович, Ю.В. Беженар, О.Г. Голубничий, Р.С. Одаренко // Науково-практичний журнал "Безпека інформації". – 2012. – № 1. – С. 37–41.

25. *Wilson P.* Vulnerability of Wireline and Cellular Telecommunications Networks to High Power Radio Frequency Fields / P. Wilson. – Darby : DIANE Publishing, 2009. – 30 p.

26. *Иксар В.* Беспроводные средства связи и безопасность / В. Иксар // Портал "Warning" [Электронный ресурс]. – Режим доступа : http : // www.warning.dp.ua/tel5.htm.

27. *Кравець О.* Підвищення ефективності криптоаналізу сучасних потокових шифрів / О. Кравець, С. Лупенко, А. Луцків // Вісн. Нац. ун-ту "Львів. Політехніка". – 2012. – № 741. – С. 240–245.

28. Проблемы защиты сетей мобильной связи и шифрования данных [Электронный ресурс]. – Режим доступа : http : // mobil.km.ua/content/view/44/63/.

29. *Гордейчик С.В.* Безопасность беспроводных систем / С.В. Гордейчик, В.В. Дубровин. – М. : Горячая линия – Телеком, 2008. – 288 с.

30. Новейшие технологии защиты телефонных переговоров. Скремблеры “Guard” [Электронный ресурс]. – Режим доступа : http : // www.skrembler.ru/.

31. Генераторы шума, глушилки и подавители. НПП “Инком-Сервис” [Электронный ресурс]. – Режим доступа : http : // www.gsmjammer.ru/.

32. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей – М. : Гостехкомиссия России, 1999. – 6 с.

Отримано 17.08.2014

Рецензент Яковенко О.В., кандидат технічних наук, старший науковий співробітник.