УДК 004.056:65.012.8(045)

Скулиш Є.Д., Корченко О.Г., Горбенко Ю.І., Пушкарьов О.І. , Соловйов О.А., Коряков І.В.

СУЧАСНІ СИСТЕМИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У роботі, на основі теоретичних досліджень авторів, представлені сучасні апаратно-програмні засоби криптографічного захисту інформації, які розроблені спільними зусиллями Держспецзв'язку, Академії СБУ, Національного авіаційного університету, Науково-впроваджувальної фірми «КРИПТОН» та Закритого акціонерного товариства «Інститут інформаційних технологій». Ці засоби дають можливість в інформаційно-телекомунікаційних системах забезпечити захист від несанкціонованого доступу державних інформаційних ресурсів, що містять інформацію з обмеженим доступом. Описано призначення та основні функції запропонованих систем і комплексів криптографічного захисту інформації.

Ключові слова: системи захисту інформації, криптографічний захист інформації, електроні ключі, криптомодуль, сертифікація ключів, генератор ключів, центр сертифікації ключів.

Відповідно до законів України "Про інформацію", "Про державну таємницю", "Про захист персональних даних", нормативних документів технічного захисту інформації та іншої нормативно-правової бази держави зростають вимоги до захисту державних інформаційних ресурсів [1]. У зв'язку з цим, створення відповідної теоретичної бази [2-5] і розробка засобів та систем безпеки інформації є актуальним напрямом наукових досліджень та практичних реалізацій. За інтеграцією зусиль Держспецзв'язку, Академії СБУ, Національного авіаційного університету, Науково-впроваджувальної фірми «КРИПТОН» та Закритого акціонерного товариства «Інститут інформаційних технологій» була створена теоретична основа, і на її базі низка технічних реалізацій, що дозволило забезпечити захист державних інформаційних ресурсів. У зв'язку з цим, метою роботи є демонстрація основних можливостей та комплексних рішень сучасних систем і комплексів криптографічного захисту інформації, створених за участі зазначених колективів.

До пристроїв захищеної передачі даних можна віднести **ТОПАЗ-8000** (рис. 1), призначений для шифрування даних, що передаються дротяними або мобільними каналами зв'язку та під'єднується в розрив з'єднання комп'ютера (або іншого термінального обладнання) і стандартного модему, підключеного до комутованих, виділених дротяних або мобільних каналів передачі даних (швидкість – до 115000 біт/с).

Рис. 1. ТОПАЗ-8000

Працює в мобільній мережі при використанні модему GSM і дозволяє організувати захищений зв'язок до 10 000 абонентів. Також підтримується віддалене підключення до мережі Ethernet. Об'єктом шифрування за ГОСТ 28147-89 є потік даних (за винятком АТ-команд інтерфейсу RS-232). Забезпечує ключову систему за методом Діффі-Хеллмана у варіанті Ель-Гамаля (довжина відкритої частини ключа 1024 біта, а сеансового – 256 біт) та реалізацію алгоритму аутентифікації. Довготривалий ключ (ДК) довжиною 512 бітів для алгоритму шифрування є однаковим для всіх пристроїв однієї мережі і зберігається в його недоступній ззовні пам'яті.

Разовий ключ (РК) вибирається з відповідного масиву і є унікальним для кожного напрямку зв'язку. По завершенні часу напрацювання старий РК (256 біт) знищується і автоматично заміняється новим. Існує кілька варіантів застосування, найскладнішим з яких є – змішана мережа, структура якої приведена на рис. 2, де демонструється можливість захищеного зв'язку як між фрагментами, так і між окремими абонентами мережі.

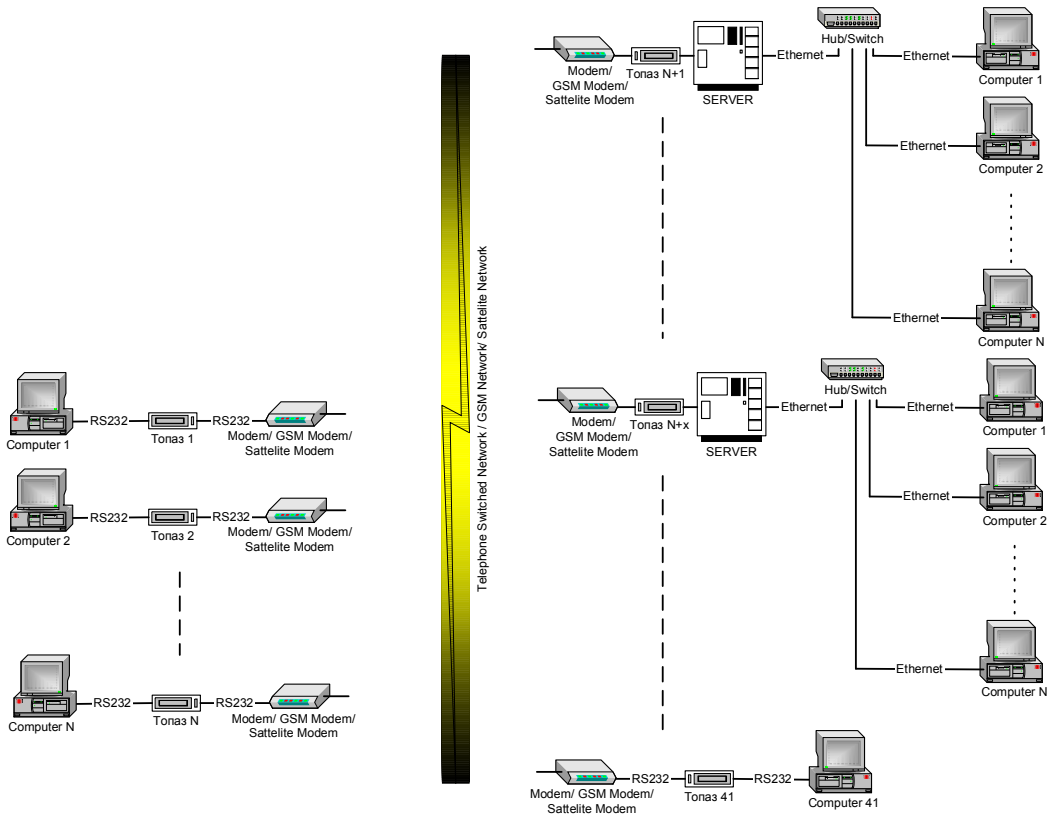


Рис. 2. Змішана мережа

Для реалізації функцій криптографічного перетворення конфіденційної інформації з обмеженим доступом (ІзОД), призначений комплекс попереднього шифрування **Кокон-М** (рис.3), який може підтримувати мережу з 256 абонентів. Модуль у складі комплексу забезпечує: криптографічне перетворення інформації відповідно до ГОСТ 28147-89 (режими – проста заміна, гамування, гамування із зворотнім зв'язком, вироблення імітовставки); генерацію та формування випадкової послідовності; неможливість зовнішнього зчитування змісту ключових даних; знищення ключових даних; перевірку працездатності та стану ключової системи; розмежування доступу до функцій за допомогою паролів. Завантаження ключових даних у модуль здійснюється за допомогою апаратно-програмного засобу формування ключів. Також забезпечена можливість «гарячої» заміни модуля, а знищення усіх даних, відкритих повідомлень та паролів, що зберігаються в оперативному запам'ятовуючому пристрої, здійснюється відразу після завершення безпосередньої роботи з ними. Комплекс має наступні режими роботи: «Самоконтроль» – перевірка цілісності програмного забезпечення (ПЗ) та наявності усіх необхідних драйверів та файлів на початку роботи; «Контроль» – автоматична перевірка працездатності модуля та ідентифікація оператора (введення паролю доступу); «Шифрування» – зашифрування та розшифрування інформації режиму встановлюється оператором за умови підключення модуля до ПК та позитивного результату в режимі «Контроль»; «Адміністрування» – знищення ключових даних, зміни паролю доступу, встановлення у початковий стан, знищення файлів даних, створення та редагування адресної книги абонентів мережі зв'язку; «Журнал» – перегляд вмісту журналу та його збереження наприкінці сеансу роботи.

Рис. 3. Кокон-М

До пристроїв криптографічного захисту в мережах передачі даних відноситься комплекс тунельного шифрування інформації у віртуальній приватній мережі (VPN) **ОНІКС 200** (рис. 4), який призначено для шифрування даних, що передаються відкритими каналами зв'язку мереж загального користування між локальними фрагментами корпоративної IP-мережі. Апарат вмикається в розрив з'єднання мультиплексного обладнання локальної і глобальної (наприклад, Інтернет) мережі. Він дозволяє створювати віртуальні приватні мережі (VPN), що містять до 1024 локальних фрагментів побудованих на базі 128 ключових напрямів зв'язку і може використовуватися для захисту конфіденційної інформації, що є власністю держави. Реалізує алгоритм шифрування ГОСТ 28147-89 за допомогою модуля апаратного шифратора Оникс-II. Обробці піддається увесь IP-пакет, що направляється абонентові мережі. Підтримується робота в мережах, що використовують технологію VLAN (IEEE 802.1Q), а пропускна спроможність пристрою до 92 Мбіт/с. Також, забезпечується віддалений контроль за роботою виробу з використанням протоколу SNMPv2c. Ключ ДК (512 біт) є однаковим для всіх пристроїв однієї віртуальної мережі і зберігається в недоступній ззовні пам'яті апаратів, а РК (256 біт) є унікальним для кожної пари абонентів мережі і вибирається з масиву відповідно до IP-адреси абонента. Відпрацьовані РК знищуються і автоматично змінюються. Введення ключової інформації здійснюється за допомогою модуля ключових даних, який є флеш-картою ММС. Структура шифратора забезпечує 100% апаратне дублювання функцій шифрування і контролю. Прийняті всі заходи для виключення неправильної роботи шифраторів, а безпека підтримується системою контролю і знищення критичної інформації як за командою оператора, так і за виявленням несанкціонованого доступу (НСД) до апаратури. Застосування цього пристрою промоделюємо на такому прикладі. Орган державної влади має свої представництва за межами країни, кожне з яких користується своєю локальною комп'ютерною мережею (3 і більше ПК) і потребує постійного взаємообміну конфіденційною інформацією. Необхідно побудувати захищену віртуальну мережу для зазначеного органу на базі технології Інтернет. Для цього у кожному представництві організується доступ до Інтернету через виділений канал і на виході локальної мережі встановлюється пристрій ОНІКС за відповідною схемою підключення (рис. 5).

Рис. 4. ОНІКС 200

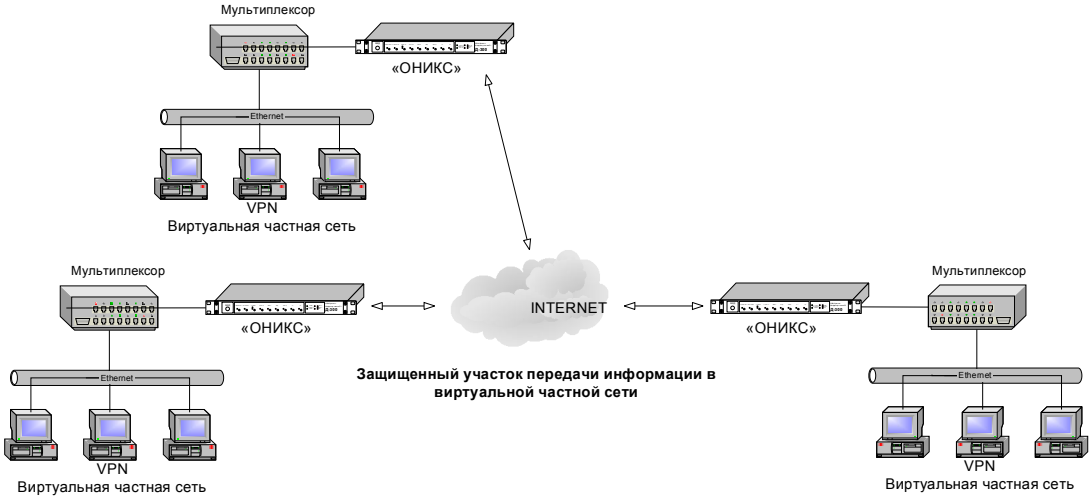
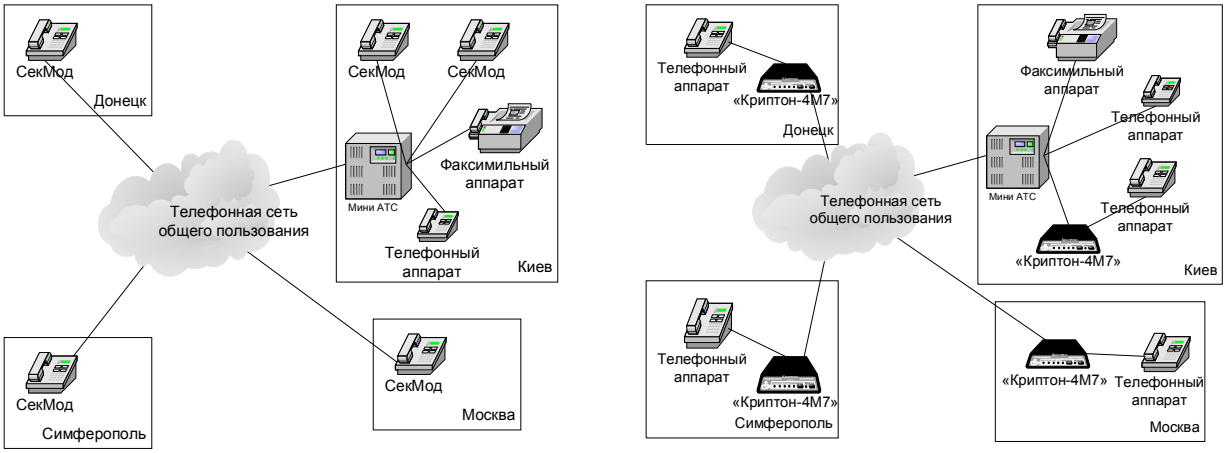


Рис. 5. Приклад застосування комплексу ОНІКС 200

Для захисту інформації, що передається комутованими каналами, використовується низка засобів, серед яких і абонентський криптографічний пристрій **СЕКМОД-К** (рис. 6), який призначено для захисту ІзОД під час передачі мовних сигналів телефонними каналами.

Рис. 6. Секмод-К

Пристрій виконано у вигляді телефонного апарату, в який вмонтовано модуль КЗІ. Він складається з таких функціональних вузлів: вокодер із швидкістю передачі даних 5600 біт/с; модуляр – криптографічний перетворювач сигналів мовного спектру; модем (рекомендації V.34, V.42) для передачі шифрованих параметрів мови між однотипними апаратами; шифратор за ГОСТ 28147-89; контролер криптопротоколу, тестів і блокувань. У пристрої реалізовано алгоритм аутентифікації та забезпечується ключова система за методом Діффі-Хеллмана у варіанті Ель-Гамаля з довжиною відкритої частини ключа 1024 біти, сеансового – 256 біт. Пристрій містить масив з 16-ти ДК довжиною 512 біт, які для кожного сеансу зв'язку вибираються випадково. Секмод-К призначений для підприємств з розгалуженою мережею дилерів у різних містах, для яких необхідно забезпечити захист телефонних переговорів. Для цього замість стандартних телефонних апаратів встановлюються криптографічні, що забезпечують як звичайні переговори так і захищені. Схема підключення – рис. 7 а.



а) б)

Рис. 7. Схеми підключення: а) СЕКМОД-К; б) Криптон-4М7

Існує і інше рішення, з використанням звичайних телефонних апаратів, в якому між телефоном і мережею загального користування (або міні-АТС) встановлюється пристрій КЗІ **Криптон-4М7**, що також і забезпечує захист передачі факсиміле.

Схема підключення – рис. 7 б. Якщо необхідно забезпечити захищеним зв'язком більше ніж двох осіб в межах офісу, то Криптон-4М7 встановлюється між міні-АТС і телефонною мережею загального користування, а організація окремої мережі рухомого зв'язку ефективно здійснюється за допомогою радіостанції **КРІОН** (видається співробітникам) із захищеним каналом.

Також, створений абонентський криптографічний пристрій **Ірпінь-2КФ** (рис. 8), призначений для захисту конфіденційної інформації, що є власністю держави під час передачі мовних сигналів телефонними комутованими каналами (фізичними лініями). За своїми криптографічними характеристиками він аналогічний пристрою Секмод-К.

Рис. 8. Ірпінь-2КФ

Розроблена низка засобів, що використовуються для криптографічного захисту цифрових потоків Е1. Пристрій **Д-300** (рис. 9) призначений для криптографічного захисту конфіденційної інформації, що є власністю держави і здійснює: приймання лінійного сигналу потоку Е1 (CEPT, PCM-30) від станційного напряму; шифрування інформації в режимі гамування відповідно до ГОСТ 28147-89; формування і передачу закритого сигналу в канал; приймання лінійного сигналу з боку каналу; розшифрування і передачу відкритого сигналу у напрямі станції. Об'єктом канального шифрування є фреймовий потік Е1, відповідний рекомендаціям ITU-T G.703, G.704, G.706, G.732, G.775, G.796, I.431 і системам з часовим розподілом ETSI ETS 300 011 (лінійний код HDB3).

Структура пристрою забезпечує 100 % апаратне дублювання функцій шифрування і контролю з можливістю реалізації зміни ключа «на льоту» (коли криптообчислювач починає роботу з новим ключем без розриву зв'язку і без втрат інформації, що передається). Для захисту одного напряму необхідно встановити два комплекти Д-300 в розрив між станційним і канальним обладнанням зв'язку.

Рис. 9. Пристрій Д-300

При щодобовій автоматичній зміні ключів комплекти можуть працювати без обслуговування протягом року. Пристрій може застосовуватися на таких ділянках захищеної системи зв'язку: підключення УАТС до центральної станції; підключення до вузла ISDN; підключення до мультиплексорів (центрам комутації); підключення до вузла супутникової системи зв'язку; зв'язок між сегментами захищеної комп'ютерної мережі. При включенні живлення виконується система тестів, зокрема стандарту FIPS 140-2. У процесі роботи проводиться тестування трактів шифрування/розшифрування і здійснюється безперервна перевірка якості каналу зв'язку. Таким чином, застосовуються всі заходи для виключення неправильної роботи. Безпека пристрою підтримується системою контролю і знищення критичної інформації як за командою оператора, так і при виявленні НСД до апаратури.

Є низка способів застосування і схем підключення спроектованих пристроїв захисту потоків Е1. Наприклад, для мережі підприємства з 80-ти комп'ютерів необхідно створити віддалений сегмент з 30 комп'ютерів із захищеною інформацією, що передається між сегментами. Для цього використовується один фреймований потік Е1 між фрагментами, два комплекти Д-300 та перетворювачів Ethernet в Е1 (наприклад, пристрої МКЕ-LAN). Після застосуванням цих засобів реальна пропускна здатність каналу між фрагментами складає 1,3-1,6 Мбіт/сек. Схема підключення наведена на рис. 10.

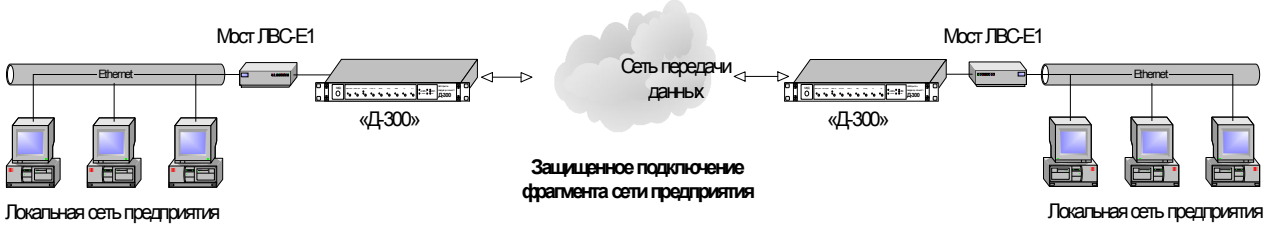


Рис. 10. Схема підключення Д-300

Для захисту факсиміле та даних, що передаються телекомунікаційними каналами з використанням УАТС можна застосовувати інше рішення, яке буде ефективним при кількості абонентів від 50 до 300 для кожної станції (див. рис. 11).

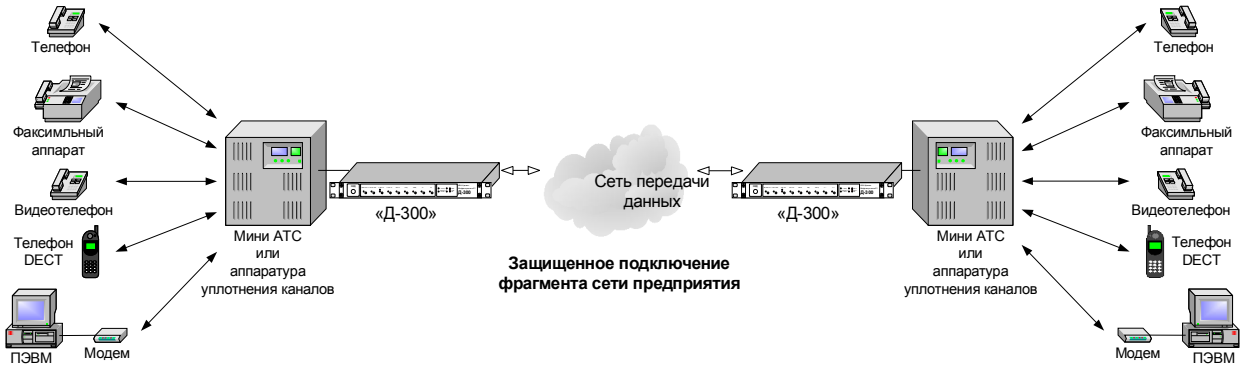


Рис. 11. Схема підключення Д-300 з використанням УАТС

Для генерації і запису ключових даних розроблено пристрій **Д-300/Ц** (рис. 12), який є автономним блоком, призначеним для формування комплекту ключів для апаратів Д-300 і записи їх в модуль ключових даних – МКД (рис. 13), виконаного у вигляді восьмиконтактного роз'ємного екранованого і герметичного з'єднувача, призначеного для транспортування ключової інформації від центру генерації ключів до апаратів КЗІ.

Модуль застосовується, як правило, в системі безпечного розподілу ключів на основі принципу “розбиття секрету”, при цьому ключова інформація транспортується в двох модулях – МКД1 і МКД2.

Рис. 12. Пристрій Д-300/Ц

Пристрій оснащений системою самотестування і контролю, яка, при щонайменших відхиленнях параметрів від норми, блокує роботу центру і виключає запис недостовірних ключових даних в МКД. У процесі роботи центру для обліку створюваних ключових документів ведется журнал подій. Конструктивно Д-300/Ц виконано у вигляді 19” блоку заввишки 1U для встановлення в стійку, а також у настільному виконанні.

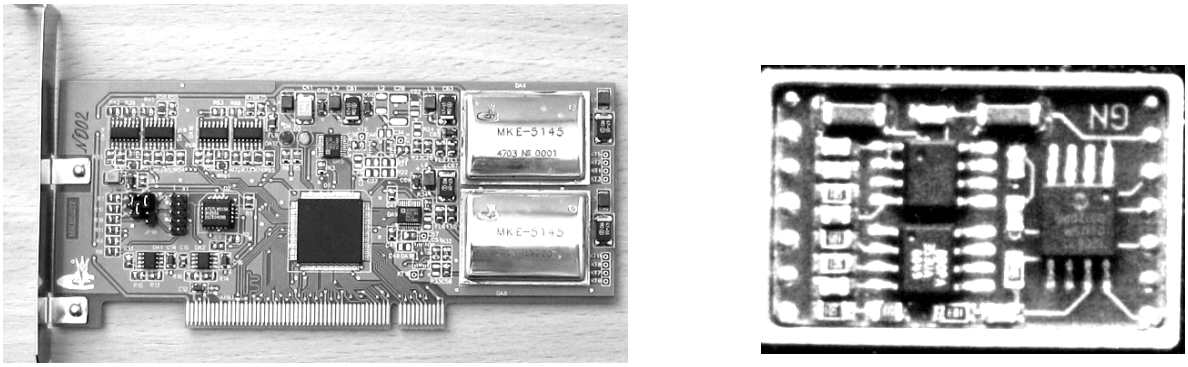
Рис. 13. МКД

Криптографічний модуль **УНІСЕК-1.Х** (рис. 14) призначений для захисту ІзОД при передачі мовних сигналів абонентськими телефонними лініями (шифрування потоку параметрів здійснюється відповідно ГОСТ 28147-89). Захисту піддається ланцюг проходження сигналу між апаратами двох абонентів, як для аналогових, так і для цифрових телефонних каналів. Модуль забезпечує ключову систему за методом відкритих ключів Діффі-Хеллмана у варіанті Ель-Гамаля (довжина відкритої частини ключа 1024 біт, сеансового – 256 біт) та реалізацію алгоритму аутентифікації. Апарат містить масив з 16-ти ДК завдовжки 512 біт, які для кожного сеансу зв'язку обираються випадково.

Модуль **УНІСЕК-2.Х** використовується для криптографічного захисту конфіденційної інформації, що є власністю держави (до корпусу терміналу пред'являються спеціальні вимоги) при передачі мовних сигналів абонентськими телефонними лініями. Пристрій за функціональним призначенням аналогічний УНІСЕК-1.Х та забезпечує ключову систему методом відкритих ключів Діффі-Хеллмана у варіанті Ель-Гамаля в групах точок еліптичної кривої, параметри якої відповідають ДСТУ 4145-2002.

Рис. 14. Модуль захисту УНІСЕК

Модуль генератора випадкових чисел МКЕ-5237 (рис. 15 а) використовується у засобах криптографічного захисту конфіденційної інформації, що є власністю держави для високопродуктивної генерації послідовностей випадкових чисел в апаратурі засобів КЗІ для формування ключових даних і випадкових параметрів криптографічних алгоритмів і протоколів (КАП). Пристрій відноситься до класу модулів розширення шини PCI та формує аналогові сигнали шуму за допомогою фізичних джерел, потужність шумового сигналу,яких перевищує потужність власних шумів і зовнішніх наведень не менше ніж на 20 дБ (окремі джерела шуму постійно контролюються на стабільність статистичних характеристик). Продуктивність модуля складає не менше 4 Мбайт/с. Пристрій МКЕ-5102 (рис. 15 б) призначений для генерації випадкових бітових послідовностей в апаратурі засобів криптографічного і технічного захисту конфіденційної інформації та відноситься до класу гібридних інтегральних мікросхем, виготовлених з використанням малогабаритних напівпровідникових приладів, безкорпусних конденсаторів і резисторів, виконаних за SMD-технологією.



а) б)

Рис. 15. Генератор випадкових чисел: а) МКЕ - 5237, б) МКЕ - 5102

Мікросхема виконана в прямокутному металосклянному корпусі типу 155-15-2 і є комбінованим аналого-цифровим пристроєм, що включає генератор аналогового шумового сигналу і мікроконтролера з вбудованим аналого-цифровим перетворювачем. Забезпечує генерацію випадкових бітових послідовностей і передачу їх зовнішнім пристроям зі швидкістю 100 Кбіт/с.

Електронний ключ (ЕК) **Кристал-1** (рис. 16) використовується для побудови апаратно-програмних засобів (АПЗ) та комплексів криптографічного захисту інформації (ККЗІ), які призначенні для захисту ІзОД в інформаційно-телекомунікаційних системах (ІТС). Виконує наступні функції: автентифікацію оператора ПК при доступі до ключа; генерацію особистих (ОК) та відкритих ключів (ВК) для алгоритму ЕЦП та протоколу

розподілу ключів; генерацію ключів для алгоритму шифрування та випадкових послідовностей на основі апаратного генератора; зберігання ОК у внутрішній пам'яті та захист їх від НСД; формування і перевірку ЕЦП; обчислення хеш-функції; розподіл ключових даних на основі асиметричного протоколу розподілу; зберігання довільних даних у внутрішній пам'яті та захист їх від НСД; контроль цілісності і працездатності вбудованого програмного забезпечення та ін. Реалізує такі КАП: шифрування за ДСТУ ГОСТ 28147:2009 (режими простої заміни та вироблення імітовставки); ЕЦП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом); хешування за ГОСТ 34.311-95; протокол розподілу ключових даних Діффі-Хеллмана у групі точок еліптичної кривої (довжина ключа ≤ 571 біт). Швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 257) – 100 мс, а спільного секрету Діффі-Хеллмана в групі точок еліптичної кривої (поле 571) – 800 мс. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до ОК з боку апаратного-програмно середовища. Генерування, зберігання, використання ОК та інших ключових даних здійснюється тільки в межах ЕК, із застосуванням його внутрішнього постійного запам'ятовуючого пристрою (ПЗП). Конструктивно ЕК виконаний у вигляді малогабаритного змінного USB-пристрою на основі двошарової друкованої плати, де встановлюються електронні компоненти і USB-з'єднувач типу A-plug (виделка) та заливається компаундом, який формує захисний шар і зовнішній вигляд виробу.

Рис. 16. Кристал-1

Апаратний модуль підпису **Гряда-41П** (рис. 17) використовується для побудови АПЗ та ККЗІ, призначених для захисту ІзОД. Функції виробу: управління ОК ЕЦП; формування ЕЦП від даних з використанням ОК; автентифікацію користувача (оператора) перед початком роботи; управління параметрами автентифікації користувачів, що включає встановлення і зміну даних автентифікації оператора; прийом, зберігання, надання доступу та знищення довільних даних у межах апаратного модуля. Реалізує вищезазначені КАП окрім протоколу розподілу ключових даних. Швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 257) – 2 мс. Апаратна реалізація забезпечує захищеність процесу формування ЕЦП та унеможливлює доступ до ОК з боку апаратного-програмно середовища. Процес генерування, зберігання та використання ОК здійснюється безпосередньо в модулі та не виходить за його межі. Для зберігання ключових даних використовується внутрішній ПЗП модуля. Виріб виконаний у конструктиві плати розширення ПК для встановлення в слот системної шини PCI-32 або PCI-X (32 біт, 33 МГц – специфікація PCI V2.1 PCISIG). Плата має багатошаровий друк з ламельним розніманням на довгій стороні для встановлення у PCI-слот ПК та USB-з'єднувачем для встановлення носіїв (ЕК) з даними автентифікації та резервними копіями ключа ЕЦП.

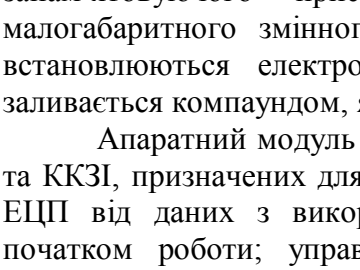


Рис. 17. Гряда-41П

Криптомодуль **Гряда-61** (рис. 18) використовується для побудови АПЗ та ККЗІ, які призначені для захисту ІзОД в ІТС. Виконує такі функції: автентифікацію оператора ПК при доступі до криптомодуля; генерацію особистих та відкритих ключів для алгоритму ЕЦП; генерацію ОК і ВК для протоколу розподілу ключів; генерацію ключів (для алгоритму шифрування) та випадкових послідовностей на основі апаратного генератора; зберігання ОК та довільних даних у внутрішній пам'яті та захист їх від НСД; шифрування даних; формування і перевірки ЕЦП; обчислення хеш-функції; розподіл ключових даних на

Рис. 18. Гряда-61

основі асиметричного протоколу розподілу; контроль цілісності і працездатності вбудованого програмного забезпечення та ін. Реалізує всі вищезазначені КАП. Швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 257) – 100 мс, а спільного секрету Діффі-Хеллмана в групі точок еліптичної кривої (поле 571) – 800 мс. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до ОК з боку апаратного-програмно середовища. Процес генерування, зберігання та використання ОК здійснюється безпосередньо в криптомодулі, та не виходить за його межі. Зберігання ОК та інших ключових даних забезпечується внутрішнім ПЗП криптомодуля. Гряда-61 виконана у вигляді малогабаритного USB-пристрою (для під'єднання до ПК за допомогою незнімного кабелю) на двошаровій друкованій платі, яка встановлена у пластиковий корпус та залита компаундом, що формує захисний шар.

Рис. 19. Гряда-211

Криптомодуль **Гряда-211** (рис. 19) використовується для побудови АПЗ та ККЗІ, які призначені для захисту ІзОД в ІТС. Виконує такі функції: автентифікацію ПК при доступі до модуля; генерацію ОК та ВК для алгоритму ЕЦП та протоколу розподілу ключів; генерацію ключів (для алгоритму шифрування) та випадкових послідовностей на основі апаратного генератора; зберігання ОК у внутрішній пам'яті та захист їх від НСД; обчислення хеш-функції, формування і перевірку ЕЦП; розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних; контроль цілісності і працездатності вбудованого програмного забезпечення та ін. Реалізує всі вищезазначені КАП. Швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 257) – 1,5 мс, а спільного секрету Діффі-Хеллмана в групі точок еліптичної кривої (поле 571) – 24 мс. Кількість формувань ЕЦП – 300 підписів/с, а спільного секрету Діффі-Хеллмана – 150 формувань/с. Апаратна реалізація забезпечує захищеність виконання усіх криптографічних перетворень в модулі та унеможливлює доступ до ОК з боку системи, у якій він використовується. Ключі ОК генеруються, зберігаються та використовуються тільки в криптомодулі, та жодним способом не потрапляють за його межі. Зберігання ОК та інших ключових даних здійснюється у ПЗП криптомодуля. Гряда-211 виконана у вигляді окремого модуля в металевому корпусі шириною 5,25 дюймів і може встановлюватися у відповідний відсік системного блоку ПК, має інтерфейси USB та Ethernet 100/1000.

Мережевий криптомодуль **Гряда-301** (рис. 20) використовується для побудови АПЗ та ККЗІ, які призначені для захисту ІзОД в ІТС. Виконує такі функції: автентифікацію ПК при доступі до модуля; генерацію ОК для алгоритму ЕЦП та протоколу розподілу ключів; генерацію ключів для алгоритму шифрування та випадкових послідовностей на основі апаратного генератора; зберігання ОК у внутрішній пам'яті та захист їх від НСД; обчислення хеш-функції, формування і перевірку ЕЦП; розподіл ключових даних на основі асиметричного протоколу розподілу та шифрування даних; контроль цілісності і працездатності вбудованого програмного забезпечення та ін. Реалізує всі вищезазначені КАП. Швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 257) – 1,5 мс, а спільного секрету Діффі-Хеллмана в групі точок еліптичної кривої (поле 571) – 24 мс. Кількість формувань ЕЦП – 1200 підписів/с, а спільного секрету Діффі-Хеллмана – 80 формувань/с. Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до ОК з боку системи. Особисті ключі генеруються, зберігаються та використовуються тільки в мережевому криптомодулі, та жодним способом не потрапляють за його межі. Зберігання ОК та інших ключових даних здійснюється у ПЗП модуля. Гряда-

Рис. 20. Криптомодуль Гряда-301

301 виконана у вигляді мережевого вузла і є системною платформою у металевому корпусі висотою 1U та призначений для встановлення в 19-ти дюймову стійку. Має мережевий інтерфейс Ethernet 10/100/1000.

Рис. 21. Гряда-4

Апаратний генератор випадкових чисел (генератор ключів) **Гряда-4** (рис. 21) використовується для побудови АПЗ та ККЗІ, орієнтованих на захист ІзОД. Призначений для апаратної генерації послідовностей випадкових чисел на основі фізичних датчиків шуму у складі АПЗ та ККЗІ, що реалізовані на основі ПК. Генератор виконаний у вигляді малогабаритного пристрою, який має кронштейн для розміщення всередині системного блоку ПК, та з'єднується з системною платою ПК через USB-інтерфейс за допомогою кабелю. Гряда-211 виконана на двошаровій друкованій платі, яка розміщена у пластиковому корпусі та нерозбірно поєднана з ним шляхом заливки компаундом. Електроживлення під'єднаного пристрою, здійснюється від блоку живлення через USB-інтерфейс.

IP-шифратори **Канал-201, Канал-301** та **Канал-401** (рис. 22) використовуються для побудови ІТС, які призначені для обробки ІзОД. Виконують такі функції: шифрування та контроль цілісності IP-пакетів, їх інкапсуляцію та маршрутизацію між мережевими інтерфейсами; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами. Реалізують всі вищезазначені КАП. Швидкість шифрування Канал-201 – 100 Мбіт/с, Канал-301 – 250 Мбіт/с, Канал-401 – 350 Мбіт/с.

а) б) в)

Рис. 22. IP-шифратори: а) Канал-201; б) Канал-301; в) Канал-401

Всі пристрої виконані у вигляді окремого мережевого вузла. Конструктивно IP-шифратори Канал-201 та Канал-301 є системними платформами у металевому корпусі висотою 1U, що можуть встановлюватись в 19-ти дюймову стійку за допомогою полки, має 2 мережевих інтерфейси Ethernet 10/100/1000, а Канал-401 – висотою 2U і має 2×2 (дубльованих) мережевих інтерфейси Ethernet 10/100/1000 (2 електричних та 2 оптичних – LC).

Рис. 23. Бар'єр-301

Шлюз захисту **Бар'єр-301** (рис. 23) використовується для побудови ІТС, які призначені для обробки конфіденційної інформації. Виконує такі функції: автентифікацію клієнтів захисту при підключенні до сервера; встановлення захищеного TCP-з'єднання з клієнтом у разі успішної автентифікації; встановлення відкритого TCP-з'єднання з сервером; прийом та розшифрування даних TCP-з'єднання від клієнта (сервера) та передача їх серверу (клієнту). Реалізує всі вищезазначені КАП. Кількість автентифікацій клієнтів – 100 автентифікацій/с, а швидкість шифрування – 250 Мбіт/с. Виконаний у вигляді окремого мережевого вузла та є системною платформою у металевому корпусі висотою 1U. Може встановлюватись в 19-ти дюймову стійку за допомогою полки, має 2 мережевих інтерфейси Ethernet 10/100/1000.

Рис. 24. Смарт-карта

Смарт-карта **Карта-1** (рис. 24) використовується для побудови АПЗ та ККЗІ, які призначені для захисту ІзОД в ІТС. Виконує такі функції: автентифікацію оператора ПК при доступі до карти; генерацію ОК і ВК для алгоритму ЕЦП для протоколу розподілу ключів; генерацію ключів (для алгоритму шифрування) та випадкових послідовностей на основі

апаратного генератора; зберігання ОК у внутрішній пам'яті та захист їх від НСД; формування і перевірку ЕЦП; обчислення хеш-функції; контроль цілісності і працездатності вбудованого програмного забезпечення та ін. Реалізує всі вищезазначені КАП, а швидкість формування ЕЦП за ДСТУ 4145-2002 (поле 191) – 200 мс. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до ОК з боку апаратного-програмно середовища. Збереження ОК та інших ключових даних, а також їх генерування здійснюється тільки усередині смарт-карти. Конструктивно виріб є малогабаритною пластиковою картою з контактною мікросхемою.

На основі зазначених засобів будуються сучасні системи ККЗІ. Для прикладу розглянемо побудову програмно-технічного комплексу центру сертифікації ключів (ЦСК), призначеного для реалізації регламентних процедур та механізмів обслуговування сертифікатів ВК користувачів, надання послуг фіксування часу, а також надання користувачам засобів шифрування та генерації ОК і ВК. Комплекс обробляє ІзОД і включає програмні та апаратно-програмні засоби КЗІ. Технічні засоби об'єднані у локально-обчислювальні мережі (ЛОМ) з використанням внутрішньої комунікаційної мережі з наявністю підключення до зовнішніх комунікаційних мереж (ЗКМ). Окремі технічні засоби ізольовані від мереж передачі даних. Порядок експлуатації комплексу у складі ЦСК відповідає вимогам правил посиленої сертифікації. Функціональна схема комплексу наведена на рис. 25.

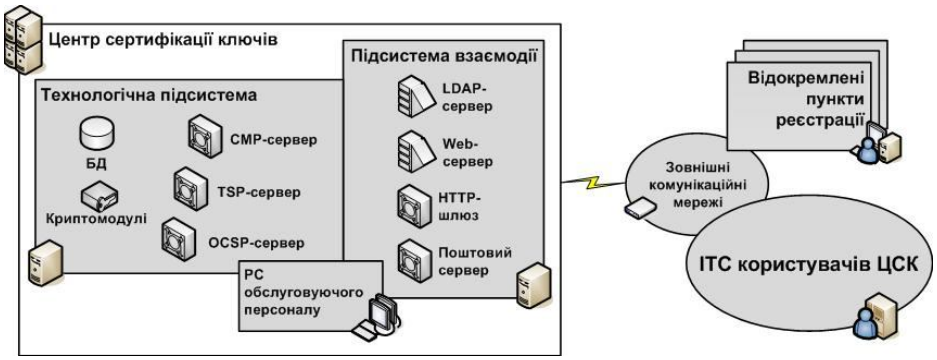


Рис. 25. Склад комплексу ЦСК

До складу комплексу входять засоби користувачів у складі: 1) засоби генерації ОК і ВК користувачів (генерація ОК та ВК користувача, формування та передача запиту на формування сертифіката користувача до ЦСК, отримання, перевірка, зберігання та використання сформованого сертифікату, формування та передача запитів на блокування, скасування та поновлення сертифіката користувача до ЦСК); 2) засоби ЕЦП та шифрування даних користувачів (введення та використання ОК користувача, пошук та інтерактивна перевірка статусу сертифікатів у ЦСК за протоколом OCSP, пошук сертифікатів у LDAP-каталозі ЦСК, отримання позначок часу у ЦСК, реалізація механізмів формування та перевірки ЕЦП, а також шифрування даних користувача у системах електронної пошти, електронного документообігу тощо).

У структуру комплексу входять такі технічні засоби (рис. 26): ПК обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та сертифікації); центральні сервери (сервери ЦСК); внутрішнє комунікаційне обладнання ЛОМ; сервери взаємодії; міжмережевий екран (МЕ) з системою попередження втручань (IDS); комунікаційне обладнання ЗКМ; ПК генерації ключів користувачів (ізольований); ПК віддалених адміністраторів реєстрації (відокремлені).

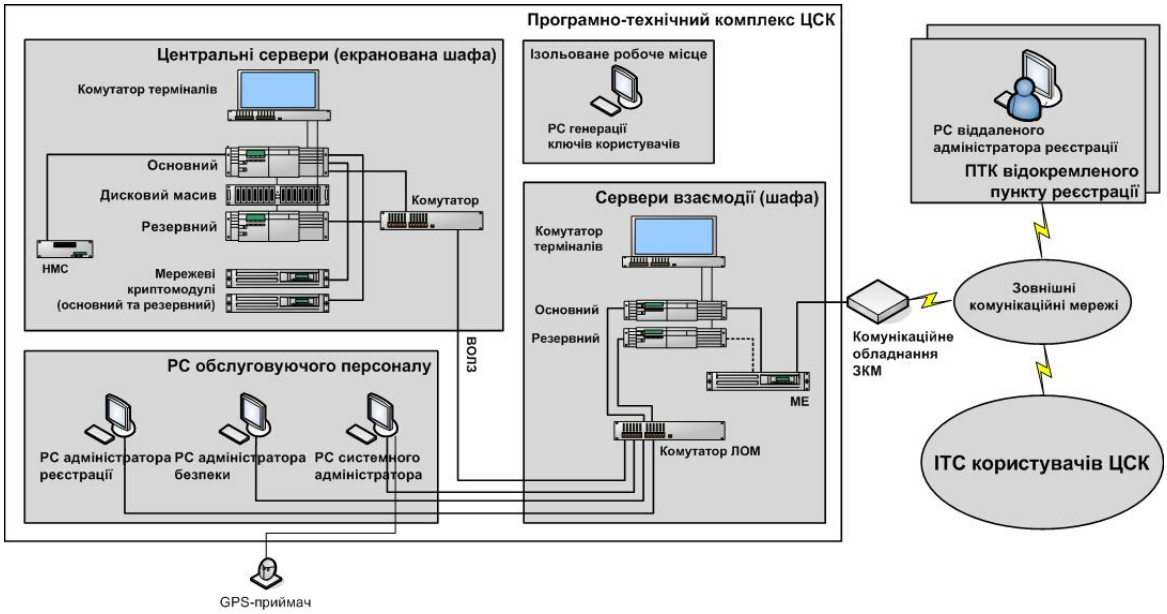


Рис. 26. Структурна схема комплексу технічних засобів

Функціональною основою комплексу є АПК, який складається зі спеціалізованих апаратних засобів та програмних комплексів КЗІ і включає: програмний комплекс ЦСК “ІІТ ЦСК-1”; апаратний модуль підпису “Гряда-41П”; мережевий криптомодуль “Гряда-301”; програмний комплекс віддаленого адміністратора реєстрації ЦСК “ІІТ ЦСК-1 (віддалений адміністратор реєстрації”); криптомодуль “Гряда-61”; програмний комплекс користувача ЦСК “ІІТ Користувач ЦСК-1”; електронний ключ “Кристал-1”. Комплекс забезпечує характеристики, що наведені у табл. 1.

Значення характеристик комплексу Таблиця 1

Показник	Значення
Кількість користувачів, яких обслуговує комплекс	не менше 1 000 000
Кількість користувачів, які можуть зареєструватися	не менше 5 000 за добу
Кількість користувачів, які одночасно мають доступ до сервера взаємодії (LDAP-каталогу та web-сторінки)	не менше 5 000
Час обробки запитів користувачів на формування, блокування, поновлення та скасування сертифікатів сервером ЦСК	не більше 1 с (не менше 100 запитів/с)
Час обробки запитів зовнішніх користувачів на визначення статусу сертифіката	не більше 1 с (не менше 500 запитів/с)
Час обробки запитів зовнішніх користувачів на формування позначки часу	не більше 1 с (не менше 500 запитів/с)

Комплекс забезпечує функціонування та можливість надавати доступ до ЦСК користувачам цілодобово 7 днів на тиждень. Центральні сервери та сервери взаємодії можуть функціонувати автоматизовано. Існує можливість роботи серверів у різних режимах – основний чи резервний з повним чи частковим дублюванням функцій. Функціональні характеристики та режими експлуатації комплексу не залежать від типів та характеристик технічних засобів (ПК, серверів та комунікаційного обладнання). Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно технічних специфікацій форматів представлення базових об’єктів національної системи ЕЦП (далі – національних технічних специфікацій); формати підписаних даних (даних з ЕЦП) – згідно відповідних національних технічних специфікацій та технічних рекомендацій RFC 5652 (PKCS#7); формати захищених даних (зашифрованих даних) – згідно відповідних технічних специфікацій форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та інформації про статус – згідно відповідних національних технічних

специфікацій та технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу – відповідних національних технічних специфікацій та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій PKCS#8 або PKCS#12.

Таким чином, розроблені апаратні засоби та засновані на них низки технічних рішень дають можливість забезпечити захист від НСД в ІТС державних інформаційних ресурсів, що містять інформацію з обмеженим доступом.

ЛІТЕРАТУРА:

1. Марущак А. Щодо поняття «інформаційні ресурси держави» / Інформаційна безпека людини, суспільства, держави. – 2009. – № 1(1). – с.11-16.

2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І.Д. Горбенко, Ю.І. Горбенко // Харків: Видавництво «Форт», 2011. – 870 с.

3. Корченко О.Г. Системи захисту інформації : Монографія / О.Г. Корченко. – К: НАУ. – 2004. – 264с.

4. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія / Ю.І. Горбенко, І.Д. Горбенко. – Х.: Видавництво "Форт", 2010. – 608 с.

5. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К.: НАУ, 2005. – 336 с.

Надійшла: 10.12.2011

Рецензент: д.т.н., проф. Конахович Г.Ф.