УДК 004.75
В. А. КОЗАЧОК, канд. техн. наук, Державний університет телекомунікацій, Київ

КОНЦЕПТУАЛЬНІ ЗАСАДИ СТВОРЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Розглянуто головні засади концепції зі створення комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах. Обґрунтовано необхідність створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, які забезпечують обробку інформації з обмеженим доступом, а також розкрито основні положення політики безпеки інформації в інформаційно-телекомунікаційних системах.

Ключові слова: комплексна система захисту інформації; інформаційно-телекомунікаційна система; технічний захист інформації; політика безпеки інформації; державна експертиза комплексної системи захисту інформації.

Вступ

Згідно з нормативними вимогами [1–4] на підготовчому етапі розроблення політики безпеки інформації в інформаційно-телекомунікаційних системах (ІТС) має формуватися концепція безпеки інформації. Концептуальні засади включають у себе загальну систему поглядів, керівних принципів, розкриваючи найважливіші напрямки гарантування безпеки інформації. Розроблення концепції відбувається після вибору варіанта концепції створюваної ІТС і виконується на підставі аналізу таких чинників:

- правових і/або договірних засад;
- вимог до гарантування безпеки інформації згідно із завданнями та функціями ІТС;
- загроз, впливу яких зазнають ресурси ІТС, що підлягають захисту.

Інформація, яка є власністю держави, або інформація з обмеженим доступом (ІзОД), вимогу щодо захисту якої встановлено законом, має оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, установленому законодавством [1; 2].

Основна частина

До складу комплексних систем захисту інформації (КСЗІ) ІТС входять заходи та засоби, які реалізують способи, методи й механізми захисту інформації від таких чинників:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
- дій із метою несанкціонованого доступу до інформації, таких як підімкнення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;
- спеціального впливу на інформацію, який може здійснюватися через формування полів і сигналів для порушення цілісності інформації або руйнування системи захисту.

Для організації робіт зі створення КСЗІ ІТС упроваджується служба захисту інформації в ІТС, порядок створення, завдання, функції, структура та повноваження якої визначено нормативними документами з технічного захисту інформації (ТЗІ) [5].

КСЗІ створюється з урахуванням забезпечення необхідного режиму обмеження доступу під час проектування, розроблення, виготовлення, випробування, сертифікації, експлуатації, ремонту, списання та ліквідації відповідних ІТС.

На об'єктах інформаційно-телекомунікаційних систем має бути розроблено необхідні документи відповідно до вимог нормативно-правових актів стосовно охорони інформації з обмеженим доступом, а також запроваджено відповідний контроль.

Мета створення КСЗІ така:

- гарантування безпеки інформації, що обробляється та зберігається в ІТС в усіх режимах їхнього функціонування, від несанкціонованого доступу, запобігання порушенням конфіденційності, цілісності, доступності, спостережуваності;
- захист ІзОД у каналах та лініях зв'язку;
- антивірусний захист інформації;
- захист ІзОД від витоку технічними каналами;
- захист інформації від спеціального впливу.

Для досягнення поставлених цілей щодо комплексного захисту інформації в ІТС передбачено:

- організаційно-правові заходи з регламентування діяльності користувачів та обслуговувального персоналу;
- організаційно-технічні заходи, а також програмні засоби захисту від несанкціонованого доступу;
- організаційно-адміністративні та організаційно-технічні заходи захисту інформації від витоку технічними каналами;

• організаційно-технічні заходи й програмно-апаратні засоби забезпечення цілісності оброблюваної інформації та ресурсів ІТС;

• організаційно-адміністративні заходи з обмеження фізичного доступу до технічних засобів обробки інформації;

• організаційні заходи та програмні засоби захисту інформації від впливу комп'ютерних вірусів.

Захист інформації в сучасних ІТС здійснюється на таких принципах:

• адміністративне та частково довірче управління доступом;

• мінімум повноважень стосовно доступу до ресурсів, що підлягають захисту;

• збереження захищеного стану інформації в разі відмови окремих складових системи;

• захист об'єктів системи захисту;

• безперервність захисту;

• комплексність захисту.

КСЗІ ІТС має створюватися згідно з вимогами нормативних документів щодо ТЗІ, являючи собою комплекс програмних і технічних засобів у поєднанні з організаційними заходами.

Аналізуючи структуру побудови сучасних ІТС, їхніх складових систем і підсистем, а також технологію обробки, збереження та передавання інформації, доходимо таких висновків.

1. До ***інформаційних ресурсів***, що підлягають захисту за вимогами забезпечення конфіденційності, цілісності, доступності та спостережуваності, належать:

• дані у вигляді електронних документів, окремих файлів, каталогів, баз даних тощо;

• бази даних захисту (списки зареєстрованих користувачів, їхні ідентифікатори, повноваження, матриці доступу, журнали реєстрації подій);

• проектно-експлуатаційні, організаційно-технічні, розпорядчі документи.

2. До ***технічних ресурсів***, що підлягають захисту, належать:

• технічні засоби та обладнання (серверне, телекомунікаційне, мережне, АРМ);

• комунікаційні засоби (локальні мережі, засоби доступу до локальних мереж, лінії та канали зв'язку);

• технічні засоби, що забезпечують обробку інформаційних ресурсів;

• допоміжне обладнання;

• спеціальні засоби інформаційного захисту.

3. До ***програмних ресурсів***, що підлягають захисту, належать:

• загальне програмне забезпечення (операційні системи, системи управління базами даних, засоби для роботи з електронними документами);

• спеціальне програмне забезпечення (пакети для підтримання електронного документообігу, обробки текстових, графічних та інших даних, засоби пошуку інформації);

• спеціалізовані засоби захисту інформації (захисту від витоку її технічними каналами, криптографічні засоби, засоби антивірусного захисту).

4. До ***фізичних ресурсів***, що підлягають захисту, належать приміщення, де розташовуються технічні ресурси, елементи обчислювальної системи, машинні носії інформації.

Згідно із [6] загрози класифікують за результатом їхнього впливу на інформацію, тобто порушенням ***конфіденційності***, ***цілісності***, ***доступності*** та ***спостережуваності*** інформації.

Необхідність і зміст заходів щодо КСЗІ визначаються можливими загрозами інформаційній безпеці, а також рівнем їх небезпечності. Як критерій оцінки небезпечності загроз розглядають рівень потенційних збитків у разі їх реалізації. Рівень збитків від впливу тієї чи іншої загрози визначається важливістю оброблюваної в ІТС інформації та ймовірністю реалізації загроз, а тому в кожній складовій системі та підсистемі ІТС зазначений рівень має оцінюватися індивідуально.

За результатами впливу на конфіденційність, цілісність, доступність та спостережуваність інформації загрози в загальному вигляді поділяються на такі види.

1. Загрози щодо порушення ***конфіденційності інформації*** внаслідок:

• неправильного керування потоками інформації;

• наявності запитів до інформаційних ресурсів із боку сторонніх осіб;

• несанкціонованого доступу (НСД) до інформаційних ресурсів під час експорту/імпорту інформації, зокрема з використанням атрибутів доступу попереднього користувача однойменних ресурсів;

• існування прихованих каналів;

• використання засобів перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН), акустоелектронних перетворень інформаційних сигналів;

• будь-яких дій, що можуть призвести до розголошення відомостей стосовно атрибутів розмежування доступу, їх втрати тощо.

2. Загрози щодо порушення ***цілісності інформації*** внаслідок:

• неправильного керування потоками інформації;

• наявності прав доступу до інформаційних ресурсів із боку сторонніх осіб;

• помилок користувачів, збоїв програмного забезпечення (ПЗ);

• ненавмисного ураження комп'ютерними вірусами;

• зміни умов фізичного середовища (вологість, коливання температури, природні явища);

• збоїв і відмов у роботі обладнання та технічних засобів.

3. Загрози щодо порушення ***доступності інформаційних ресурсів*** унаслідок:

• проведення модернізації ІТС (програмних або апаратно-програмних засобів);

• відмови ІТС або переривання обслуговування.

4. Загрози щодо порушення ***спостережуваності інформації*** внаслідок:

• НСД до даних реєстраційних журналів; неавторизованого входу в ІТС;

• використання сторонніми особами атрибутів доступу до ІТС інших користувачів;

• порушення безпеки інформації в разі необережної взаємодії користувачів і КСЗІ;

• неавторизованих дій користувачів, зумовлених надмірно високими можливостями в плані адміністрування ІТС;

• порушення безпеки інформації внаслідок неправильного функціонування КСЗІ.

Дії порушників можуть призвести до виникнення таких загроз:

• використання з корисливою метою (шантаж, підкуп тощо) персоналу об'єкта;

• викрадення носіїв інформації, виробничих відходів (роздруківок, записів тощо);

• несанкціонованого копіювання носіїв інформації;

• вчинення будь-яких дій, що можуть призвести до розголошення ІзОД, атрибутів розмежування доступу, втрати атрибутів;

• порушення режимів функціонування (виведення з ладу) систем життєзабезпечення об'єкта (електроживлення, заземлення, охоронної сигналізації, вентиляції тощо);

• навмисного пошкодження носіїв інформації;

• порушення фізичної цілісності об'єкта захисту (окремих компонентів, пристроїв, обладнання, носіїв інформації);

• порушення режимів функціонування об'єкта захисту (обладнання та програмного забезпечення);

• упровадження і використання програмних вірусів, закладних (апаратних і програмних) пристроїв ЕОМ, зовнішніх нагромаджувачів;

• отримання атрибутів доступу з подальшим їх використанням для маскування під зареєстрованого користувача («маскарад»);

• неправомірного підімкнення до каналів зв'язку, перехоплення передаваних даних, аналізу трафіку тощо;

• упровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації;

• неправомірних змін режимів роботи об'єкта (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестувальних або технологічних процесів, які можуть призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

• ненавмисного ураження ПЗ комп'ютерними вірусами;

• невиконання організаційних вимог чинних на об'єкті розпорядчих документів;

• помилок при введенні даних у систему за неправильними адресами;

• неправомірного впровадження та використання забороненого політикою безпеки ПЗ (навчальні, ігрові програми, системне та прикладне забезпечення тощо);

• некомпетентного застосування засобів захисту.

Моделі загроз і порушників є вихідними даними для вибору профілів захищеності та відповідних послуг для усунення загроз інформаційній безпеці.

Політика безпеки інформації в ІТС, її складових систем і підсистем має забезпечувати:

• конфіденційність, цілісність, доступність та спостережуваність інформації при створенні та експлуатації ІТС;

• своєчасну та ефективну нейтралізацію загроз інформації та ресурсам на основі комплексного впровадження правових, організаційних, технічних, програмно-апаратних заходів і засобів захисту;

• розмежування доступу користувачів до інформації та інших ресурсів ІТС;

• реєстрацію спроб реалізації загроз інформації, оперативне оповіщення про факти несанкціонованих дій з інформацією;

• контроль за підтриманням цілісності критичних ресурсів КСЗІ, середовища виконання прикладних програм;

• забезпечення управління засобами КСЗІ та контролю за їх функціонуванням;

• створення умов для своєчасної та ефективної локалізації шкоди, якої можуть завдати несанкціоновані дії порушників політики безпеки, впливи зовнішнього середовища та інші чинники.

В основу політики безпеки має бути покладено адміністративний принцип розмежування доступу, який реалізується згідно з принципом мінімуму повноважень, тобто коли право доступу до захищених ресурсів може бути надане лише в разі службової необхідності. У рамках окремої системи або підсистеми ІТС адміністративний принцип розмежування доступу може, при потребі, доповнюватися довірчим, який реалізується в колі користувачів з однаковими повноваженнями. Порядок розмежування доступу має закріплюватися відповідними документами (інструкціями, положеннями тощо), в яких встановлюються правила класифікації інформації та користувачів, правила надання користувачам повноважень,

атрибутів і прав доступу, правила розмежування доступу.

Вимоги до функціональних профілів захищеності інформації, а також до реалізації послуг безпеки в окремих складових ІТС мають реалізуватися за єдиними принципами в рамках єдиної політики безпеки інформації.

Типові компоненти КСЗІ одного рівня мають бути оснащені функціонально однаковими механізмами реалізації. В основу інформаційного забезпечення та технології обробки у складових системах і підсистемах ІТС покладено єдність поглядів на створення організаційно-функціональних структур, апаратно-програмного забезпечення, стандартизації та уніфікації технічного обладнання, єдині правила організації документообігу.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення та впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, установленими нормативно-правовими актами та нормативними документами у сфері захисту інформації [1; 2].

Процес створення КСЗІ в ІТС розглядається як сукупність упорядкованих у часі, взаємозв'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне та достатнє для створюваної КСЗІ [3; 4].

Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ має бути узгоджено з відповідними стадіями й етапами робіт зі створення ІТС.

Дозволяється вилучати окремі етапи робіт або поєднувати кілька етапів, а також включати нові етапи робіт. При потребі дозволяється змінювати послідовність виконання окремих етапів — виконувати одночасно кілька етапів робіт, окремі етапи виконувати до завершення попередніх і т. ін., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

Розробка КСЗІ ІТС має здійснюватись згідно з такими принципами:

- КСЗІ розглядається як складова ІТС та всіх її компонентів;
- захист інформації забезпечується на всіх етапах життєвого циклу ІТС — від її розробки до утилізації включно;
- етапи створення КСЗІ в частині формування вимог, розробки політики безпеки інформації в ІТС, технічного завдання на КСЗІ, проекту КСЗІ, а також уведення в дію та оцінювання захищеності мають узгоджуватися з відповідними етапами створення ІТС;
- замовник і розробник ІТС мають виступати і як замовник, і як розробник КСЗІ;
- у разі потреби розробник ІТС, за погодженням із замовником, може для виконання робіт зі створення КСЗІ залучати інші організації, які мають необхідні ліцензії (дозволи) на проведення таких робіт;
- замовниками КСЗІ конкретних підсистем (елементів тощо) ІТС є органи управління, в інтересах яких ведеться розробка підсистеми;
- фінансування створення КСЗІ має бути передбачено за рахунок коштів, що виділяються на розробку ІТС (її складових, підсистем, елементів тощо), і становити 20–30% від загальних обсягів фінансування.

Етапи створення КСЗІ [4]:

1. Формування загальних вимог до КСЗІ в ІТС, які включають у себе:
- обґрунтування необхідності створення КСЗІ;
- обстеження середовищ функціонування ІТС;
- формування завдання на створення КСЗІ.

2. Розробка політики безпеки інформації в ІТС:
- вивчення об'єкта, на якому створюється КСЗІ;
- вибір варіанта КСЗІ;
- оформлення політики безпеки.

3. Розробка технічного завдання на створення КСЗІ.

4. Розробка проекту КСЗІ.

5. Введення КСЗІ в дію та оцінювання захищеності інформації в ІТС:
- підготовка КСЗІ до введення в дію;
- навчання користувачів;
- комплектування КСЗІ;
- будівельно-монтажні роботи;
- пусконалагоджувальні роботи;
- попередні випробування;
- дослідна експлуатація;
- державна експертиза КСЗІ (окремий етап приймальних випробувань ІТС).

6. Супроводження КСЗІ.

Порядок створення КСЗІ поширюється і на складові (або їх сукупність) КСЗІ інтегрованих ІТС.

Інтегрована ІТС за своїм складом і структурою, функціональними завданнями, можливими суттєвими відмінностями середовищ функціонування кожної складової ІТС та іншими характеристиками може бути неоднорідною системою. Для кожної окремої системи у складі такої ІТС існують тільки їй притаманні критичні інформаційні ресурси, програмно-апаратні засоби обробки даних, архітектура обчислювальної системи, особливості середовища користувачів та технології обробки інформації, канали обміну інформацією, перелік конкретних загроз тощо. Саме тому вимоги до політики безпеки інформації, функціонального профілю захищеності інформації, а також до реалізації послуг безпеки в різних складових ІТС на різних об'єктах, де будуть розгортатися її компоненти, мають бути різні.

З огляду на сказане КСЗІ інтегрованої ІТС доцільно будувати за модульним принципом (коли кожна достатньо незалежна складова частина ІТС має свій власний модуль КСЗІ, а КСЗІ інтегрованої ІТС являє собою сукупність усіх модулів, взаємодія яких забезпечується окремою підсистемою взаємодії та обміну інформацією, єдиною для всієї КСЗІ ІТС. Вибір заходів і механізмів захисту кожного модуля здійснюється відповідно до політики безпеки інформації в ІТС та концепції побудови КСЗІ ІТС, чим забезпечується їх узгодження між собою.

Такий підхід має на меті забезпечити:

• реалізацію відкритої архітектури безпеки, зміст концепції якої подано в ISO 7498-2-89. Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture;

• можливість незалежної розробки, упровадження, проведення випробувань та експлуатації кожної складової КСЗІ окремо;

• уніфікацію та здешевлення процедури проектування КСЗІ, яка зрештою зводиться до проектування певної кількості типових компонентів, кожний з яких має лише свої власні дані (для формування бази даних захисту), а не механізми захисту;

• можливість оцінювання кожної складової частини КСЗІ окремо (для будь-якого виду випробувань).

Отже, для кожного з ієрархічних рівнів інтегрованих ІТС визначаються типові (уніфіковані) варіанти (модулі) щодо реалізації підсистем КСЗІ. Кількість таких варіантів має бути мінімізована.

Обмін ІзОД між окремими типовими елементами має здійснюватися в зашифрованому вигляді або захищеними каналами зв'язку, відповідно до вимог законодавства з питань технічного та криптографічного захисту інформації.

Що ж до інтегрованих ІТС, то в них спільними ресурсами можуть бути загальносистемне ПЗ та окремі ресурси ІТС (сервери, спеціальне ПЗ).

Криптографічні засоби захисту інформації мають реалізовуватися з дотриманням вимог Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22.05.98 року № 505/98, Положення про порядок розроблення, виготовлення, введення в експлуатацію та експлуатацію засобів криптографічного захисту інформації, затвердженого наказом ДСТСЗІ СБ України від 28.02.00 року № 014, Закону України «Про електронний цифровий підпис», затвердженого Президентом України від 22.05.03 року № 852-VI.

При супроводженні КСЗІ ІТС мають виконуватися роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до планів захисту та експлуатаційної документації на компоненти КСЗІ, а також гарантійного та післягарантійного технічного обслуговування засобів захисту інформації.

Висновки

Оцінювання захищеності інформації, яка обробляється або циркулює в складових ІТС, відбувається за допомогою державної експертизи КСЗІ, яка є власністю держави або захист якої гарантується державою [7].

Для інтегрованих ІТС може проводитись державна експертиза кожної складової (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІТС полягає в перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів.

Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним технічним завданням, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться в повному обсязі експертиза одного обраного типового модуля, а на другому здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об'єкті для всіх модулів КСЗІ цього типу.

При введенні до складу діючої КСЗІ нового (оціненого) модуля повторної експертизи всієї КСЗІ не проводять. Оцінюванню підлягає взаємодія нового модуля зі складовими КСЗІ, які вже перебувають в експлуатації.

Приймальні випробування ІТС проводяться за умови, що в її складі функціонує КСЗІ. При цьому використовуються тестові дані, які не містять ІзОД.

Література

*1. **Закон України** «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94 № 81/94ВР.*

*2. **Постанова** КМ України № 373 від 29.03.06 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».*

*3. **ДСТУ 3396.1–96**. Захист інформації. Технічний захист інформації. Порядок проведення робіт.*

*4. **НД ТЗІ 3.7–003–05**. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній*

системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 8 листопада 2005 р. № 125.

5. ***НД ТЗІ 1.4–001–2000.*** *Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53.*

6. ***НД ТЗІ 1.1-002-99.*** *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.*

7. ***Положення*** *про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 р. № 62.*

В. А. Козачок

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ СОЗДАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Рассмотрены основные положения концепции по созданию комплексных систем защиты информации в современных информационно-телекоммуникационных системах. Обоснована необходимость создания комплексных систем защиты информации в информационно-телекоммуникационных системах, обеспечивающих обработку информации с ограниченным доступом, а также раскрыты основные положения политики безопасности информации в информационно-телекоммуникационных системах.

Ключевые слова: комплексная система защиты информации; информационно-телекоммуникационная система; техническая защита информации; политика безопасности информации; государственная экспертиза комплексной системы защиты информации.

V. A. Kozachok

CONCEPTUAL BASES OF CREATION COMPLEX INFORMATION SECURITY SYSTEMS IN THE INFORMATION AND TELECOMMUNICATIONS SYSTEMS

The main provisions of the concept to create a comprehensive information security systems in modern information and telecommunication systems. The necessity of creation of complex information security systems in information and telecommunication redundant system in which information is processed with limited access. Substantiated the main provisions of the security policy information in the information and telecommunication redundant system..

Keywords: complex system of information protection; information and telecommunications system; technical information security; information security policy; state expertise of complex information protection system.

УДК 621.396.967.2

А. О. ЛУНТОВСЬКИЙ, д-р техн. наук, професор, БЕРУФС Академія, Дрезден;
А. І. СЕМЕНКО, д-р техн. наук, професор, Державний університет телекомунікацій, Київ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ SDN ДЛЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ПРОВАЙДЕРСЬКОГО ЯДРА СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G МАЙБУТНЬОГО ПОКОЛІННЯ

Розглянуто особливості програмно-конфігурованих мереж SDN, в яких функції передавання трафіку відокремлено від функцій управління мережею. Обґрунтовано доцільність та ефективність використання технологій SDN при створенні систем мобільного зв'язку майбутнього покоління 5G за стандартом IMT 2020.

Ключові слова: програмно-конфігуровані мережі; системи мобільного зв'язку 5-го покоління; функції передавання трафіку; функції управління.

Віртуалізація ресурсів та програмно-конфігуровані мережі

Програмно-конфігурована мережа (***Software-Defined Networking — SDN***) — це віртуалізована мережа для передавання даних, в якій шар менеджменту (контролю або управління) мережею (*Management Plane*) відокремлений від пристроїв передавання даних і реалізується програмним шляхом. SDN являє собою одну з відомих форм віртуалізації обчислювальних ресурсів, зокрема мережних сервісів і додатків (рис. 1). Принципи створення зазначених мереж сформулювали в 2006 році фахівці всесвітньо відомих університетів Берклі та Стенфорда.