УДК 004.056.5

Шевченко В.Л., д.т.н., с.н.с.[1];
Берестов Д.С.[2];
Зотова І.Г.[2]

[1] - Державний університет телекомунікацій;
[2] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

Вибір моделі побудови інфраструктури відкритих ключів

Резюме. Розглядаються аспекти впровадження інфраструктури відкритих ключів, як основного механізму забезпечення функцій захисту інформаційно-телекомунікаційної системи.

Ключові слова: інформаційно-телекомунікаційна система, центр сертифікації ключів, інфраструктура відкритих ключів, електронний цифровий підпис.

Выбор модели построения инфраструктуры открытых ключей

Резюме. Рассматриваются аспекты внедрения инфраструктуры открытых ключей, как основного механизма обеспечения функций защиты информационно-телекоммуникационной системы.

Ключевые слова: информационно-телекоммуникационная система, центр сертификации ключей, инфраструктура открытых ключей, электронная цифровая подпись.

Model construction public key infrastructure

Resume.. Are discussed aspects of the implementation of public key infrastructure as the main mechanism to ensure the protection functions of information and telecommunications system.

Keywords: Information and Telecommunications System, Certification authority, Public Key Infrastructure, Digital Signature.

Постановка проблеми. На етапі переходу Збройних Сил України від заходів реформи до планового будівництва, всебічного нарощування потенціалу всіх складових, опрацювання Державної програми будівництва та розвитку Збройних Сил України гостро постає питання розбудови інформаційно-телекомунікаційної системи Збройних Сил України. Особливої гостроти ця проблема набуває у зв'язку з побудовою Єдиної автоматизованої системи управління Збройних Сил України – це породжує серйозні супутні проблеми.

Однією з таких супутніх проблем є надійний захист інформації, що циркулює в системах обробки, який забезпечував би попередження перекручування або знищення інформації, а також її зловмисне отримання, використання або несанкціоновану модифікацію. Забезпечення та підтримання зазначених властивостей інформації в системі потребують ідентифікації суб'єктів відносин і забезпечення цілісності та достовірності інформації з використанням електронного цифрового підпису (ЕЦП). На світовому рівні та в усіх технологічно розвинутих державах застосування цифрового підпису під час обробки інформації є усталеною практикою.

Законодавством України визначено правовий статус електронного цифрового підпису та електронного документа [1, 2], введено у дію національний стандарт України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка". Для забезпечення використання електронного підпису необхідно впровадити інфраструктуру центрів сертифікації ключів (ЦСК). Ця інфраструктура також має загальновизнану назву інфраструктури відкритих ключів [3] (ІВК). У Законі України "Про електронний цифровий підпис" [1] та постанові Кабінету Міністрів України [2] визначено загальні функції та встановлено загальні вимоги до ЦСК.

Аналіз останніх досліджень і публікацій. У [4, 5] розглянуті моделі побудови та питання інформаційної безпеки і ризиків національної інфраструктури відкритих ключів при її реалізації для електронного уряду, державних та комерційних структур та їх

установ.

Метою статі є розгляд різних видів ієрархій ІВК та ризиків від їх реалізації.

Виклад основного матеріалу. Ключовим аспектом впровадження ІВК є вибір її архітектури та проектування. ІВК допускає гнучкість проектування незалежно від обраної технології. Етап проектування забирає тривалий час, тому що на цьому етапі повинна бути сформована політика ІВК, задана її архітектура, визначені апаратні та програмні засоби підтримки інфраструктури, обрані її компоненти, сервіси, режими роботи, протоколи та базові стандарти.

Вибір архітектури повинен починатися з вигляду ієрархії ЦСК. Кількість і рівні ЦСК повинні враховуватись відразу, залежно від вимог до безпеки і доступності.

Хоча теоретично можливо використання одного ЦСК в якості кореневого та такого що видає одночасно, однак така конфігурація небажана с точки зору безпеки та подальшої масштабованості інфраструктури. Необхідно спланувати багаторівневу структуру ЦСК.

Коли існує потреба тільки в базовому наборі криптографічних сервісів і кількість облікових записів невелике, то необхідно скористатися однорівневою ієрархією. Кореневий ЦСК не видаляється з мережі і завжди доступний для видачі сертифікатів. Керування однорівневою ієрархією не буде складним, тому що в цьому випадку використовується схема тільки з одним сервером. Недоліками подібного рішення є низька відмовостійкість та неналежний рівень безпеки. Вихід із ладу сервера приводить до неможливості обробки запитів на видачу, відновлення, відкликання сертифікатів. Компрометація єдиного сервера сертифікатів, приводить до втрати всієї ІВК, таким чином, вважаються недійсними всі сертифікати інфраструктури.

Ієрархія, що полягає із двох рівнів являє собою відключений кореневий сервер і один або декілька серверів що видають сертифікати (рис. 1.)

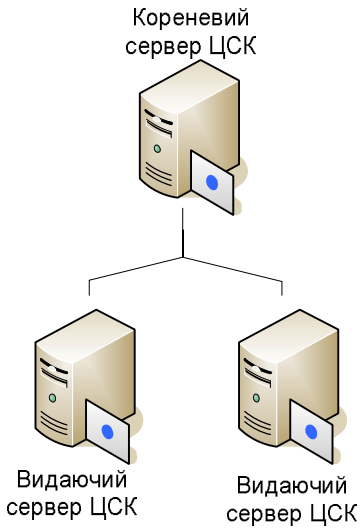

Рис. 1. Дворівнева ієрархія PKI

При цьому на видаючи ЦСК полягає функціонал по управлінню політиками сертифікатів. Для забезпечення безпеки інфраструктури кореневий центр є окремим і автономним, тобто не входить до складу домену та не підключається до локальної обчислювальної мережі, постійно перебуває у відключеному стані. Тим самим, ми уникаємо атак на кореневий сервер. Що стосується центрів, що видають, то вони одержують сертифікат, підписаний кореневим сервером, якому довіряють усі учасники взаємодії, тобто власники сертифікатів, отриманих із будь-якого ЦСК.

Для підвищення рівня доступності та відмовостійкості сервісу передбачається розгортання більш ніж одного сервера, що видає. Що стосується кількості центрів, що видають, то воно визначається функціональними вимогами покладеними на ІТС.

Трирівнева архітектура забезпечує найкращі характеристики безпеки та масштабованості інфраструктури. У цьому варіанті здійснюється розгортання кореневого центру на окремому сервері, що не входить до

складу корпоративної мережі.

Додатково виконується впровадження серверів політик, що є підлеглими до кореневого ЦСК. Ці сервери, також, не входять до складу корпоративної мережі, і є окремими. І кореневий, і підлеглі йому сервери політик, є відключеними. Сервери, що видають сертифікати, є підлеглими до сервера політик і можуть бути як корпоративними, так і окремими (рис. 2).

Рекомендується використовувати трирівневу архітектуру в наступних ситуаціях:

високі вимоги до безпеки (за рахунок використання відключених ЦСК, вдається уникнути мережевих атак);

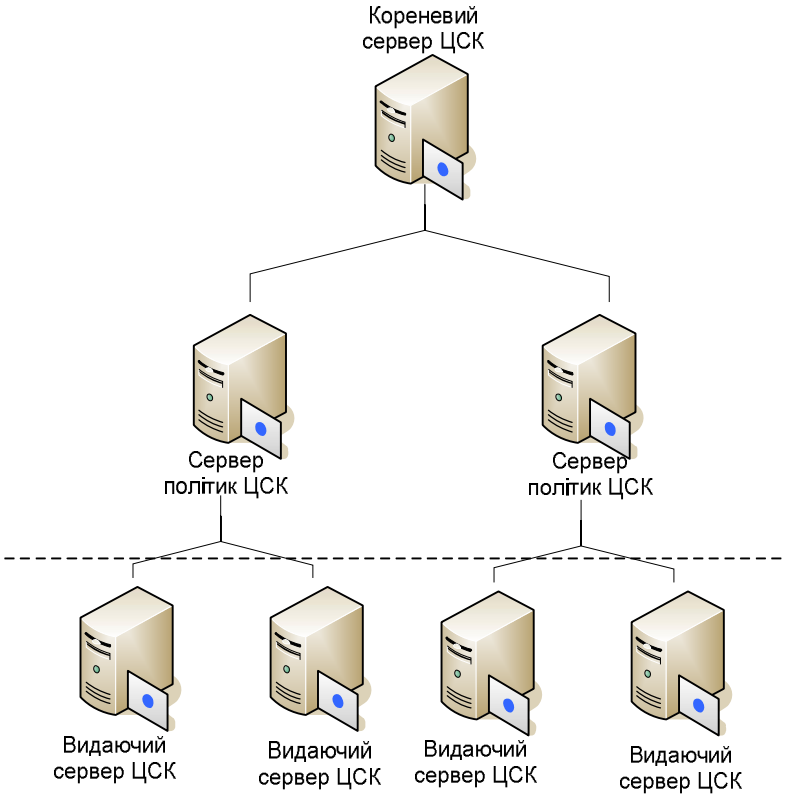

Рис. 2. Трирівнева ієрархія PKI

існує потреба в різних політиках сертифікатів та пред'являються різні вимоги до використовуємих сертифікатів;

є необхідність у роздільному керуванні (підтримка ЦСК і керування сертифікатами).

У ряді випадків може знадобитися більш складна модель, що полягає з 4-х рівнів ієрархії. Приклад такої моделі показаний на рис. 3, однак, слід мати на увазі, що такий варіант архітектури більш складний у реалізації. Реалізація моделей, що містять більш, ніж чотири рівні, не рекомендується через її надлишкову складність і неочевидної корисності.

Висновок. У статті проаналізовано ключовий аспект при впровадженні ІВК – вібір її архітектури та ризики при її реалізації.

Вибір архітектури ІВК визначається виходячи з наступних факторів:

кількість сертифікатів, які видаються;

вимоги доступності для користувачів;

модель адміністрування інфраструктури відкритих ключів;

організаційна структура.

Впровадження ІВК дозволить:

впровадити новітні інформаційні технології електронного документообігу у практику повсякденної діяльності;

розширити можливість інтеграції існуючих ІТС;

забезпечити цілісність та автентичність інформації, представленої в електронному вигляді, а також неспростовність суб'єктів інформаційних відносин;

забезпечувати легітимний електронний документообіг та реалізувати правові відносини такі, як при використанні традиційних паперових документів.

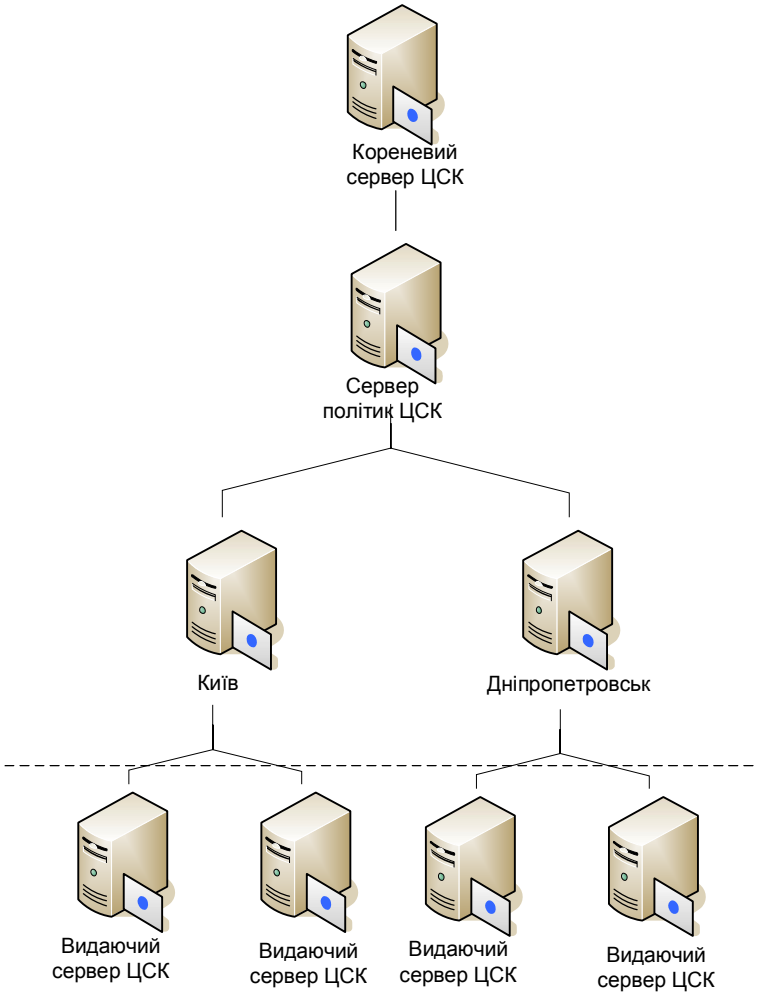

Рис. 3. Чотирирівнева ієрархія ІВК

СПИСОК ЛІТЕРАТУРИ

1. Закони України «Про електронний цифровий підпис» №852-IV від 22.05.2003, «Про електронний документообіг» №851-IV від 22.05.2003.
2. Постанови КМУ «Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу» №680 від 26.052004 р., «Порядок акредитації центру сертифікації ключів» №903 від 13.07.2004 р.
3. *D.R. Kuhn, V.C. Hu, W.T. Polk, S.J. Chang.* Introduction to Public Key Technology and the Federal PKI Infrastructure. - NIST SP 800-32, February 2001
4. *М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных, А.В. Потий* Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий. [Режим доступу] *http://www.bezpeka.com/files/lib_ru/239_bgchpopenkey.zip*
5. *С. В. Бєлов, С. В. Мартиненко* Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики [Режим доступу] *http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf*