Юрченко Юрій Юрійович, старший викладач
Жуков Роман, здобувач вищої освіти
Державний торговельно-економічний університет, Київ
ORCID: https://orcid.org/0000-0002-8047-7647 (Юрченко Ю. Ю.)
ORCID: https://orcid.org/0009-0002-0783-8618 (Жуков Р.)

**ІНФРАСТРУКТУРА ПУБЛІЧНИХ КЛЮЧІВ (PKI) У КОРПОРАТИВНИХ МЕРЕЖАХ: ЗАХИСТ, АВТЕНТИФІКАЦІЯ ТА УПРАВЛІННЯ СЕРТИФІКАТАМИ**

У сучасних корпоративних мережах захист даних і автентифікація є критичними через зростання обсягів даних і хмарних технологій. Інфраструктура публічних ключів (PKI) забезпечує надійний механізм ідентифікації, шифрування та управління доступом через цифрові сертифікати, які пов’язують відкритий ключ із власником.



Рис. 1. Схема КРІ

### *Основні елементи PKI*

PKI включає:

* Центр сертифікації (CA) — видає та підписує сертифікати.
* Реєстраційний центр (RA) — перевіряє особу заявника.
* Сховище сертифікатів — зберігає сертифікати (наприклад, LDAP).
* CRL/OCSP — перевіряє чинність сертифікатів.

### *Функціональні можливості*

PKI забезпечує:

* Цифровий підпис для автентичності документів.
* Шифрування для захисту даних.
* Автентифікацію користувачів і пристроїв.
* Контроль доступу на основі сертифікатів.

### *Застосування у корпоративних мережах*

PKI застосовується для:

* Захисту електронної пошти (S/MIME).
* VPN-з’єднань (IPSec/SSL).
* Автентифікації на веб-порталах.
* Електронного документообігу.

### Сучасні тенденції

PKI як послуга (PKIaaS) від провайдерів (Microsoft Intune, AWS Private CA) автоматизує управління сертифікатами. У IoT PKI забезпечує безпечну автентифікацію пристроїв.

### Виклики та перспективи

Впровадження PKI у корпоративних мережах пов’язане з низкою викликів. По-перше, висока вартість розгортання: створення власного CA, інтеграція з існуючими системами та навчання персоналу можуть коштувати десятки тисяч доларів, що є бар’єром для малих і середніх підприємств. По-друге, складність управління великою кількістю сертифікатів: у розподілених мережах із тисячами користувачів і пристроїв виникають проблеми з їх своєчасним оновленням і відкликанням. Наприклад, якщо сертифікат одного з пристроїв IoT скомпрометовано, затримка в оновленні CRL може призвести до вразливостей. По-третє, залежність від інфраструктури: перебої в роботі серверів OCSP або LDAP можуть зупинити перевірку сертифікатів, що вплине на доступ до критичних систем.

### Висновки

PKI є ключовим інструментом для безпеки корпоративних мереж, забезпечуючи шифрування, автентифікацію та контроль доступу. Розвиток PKIaaS і IoT розширює її можливості, але вимагає адаптації до нових викликів.

**Література**

1. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile : [RFC 5280] / IETF. – 2008. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc5280.
2. Чапля О. Системи PKI та їх застосування в ІТ-безпеці / О. Чапля // Захист інформації. – 2020. – № 2. – С. 34–41.
3. Public Key Infrastructure / Microsoft Docs. – Режим доступу: https://learn.microsoft.com/en-us/windows-server/security/public-key-infrastructure/.
4. Rescorla E. SSL and TLS: Designing and Building Secure Systems. – Addison-Wesley, 2001. – 512 с.
5. Лук’янець С. М. Безпечний обмін інформацією в корпоративних мережах / С. М. Лук’янець. – К. : ДІА, 2018. – 180 с.