АТ "Інститут інформаційних технологій"

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Комплекси та засоби криптографічного захисту інформації

Адреса: м. Харків, вул. Бакуліна, 12
Тел./факс: (057) 714-22-05
Web-сайт: iit.com.ua
E-mail: iit@iit.kharkov.ua

Про компанію

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Акціонерне товариство “Інститут інформаційних технологій” спеціалізується на наданні послуг в області проектування, розробки і впровадження рішень щодо **забезпечення безпеки інформації** у інформаційно-телекомунікаційних системах різного призначення та різного рівня складності.

Компанія має ліцензію Держспецзв’язку України від 15.02.2017 р. на провадження господарської діяльності з надання послуг у галузі **криптографічного та технічного захисту інформації** (у тому числі і інформації, що становить **державну таємницю**).

У складі компанії створені дві групи експертів, що здійснюють **експертні дослідження комплексів і засобів криптографічного захисту інформації, комплексів технічного захисту інформації та засобів захисту від НСД.**

Компанія має дозвіл на здійснення діяльності, яка пов'язана з державною таємницею.

Основні напрямки діяльності компанії

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Захист інформації у інформаційно-телекомунікаційних системах:

- створення комплексних систем захисту інформації (КСЗІ);
- розробка та впровадження комплексів і засобів криптографічного захисту інформації (КЗІ);
- впровадження засобів захисту від несанкціонованого доступу (НСД);
- створення засобів та комплексів технічного захисту інформації (ТЗІ).

Експертиза та аудит інформаційної безпеки:

- спеціальні дослідження комплексів технічного захисту інформації;
- експертиза комплексних систем захисту інформації та аудит інформаційної безпеки.

Один із напрямків діяльності - **створення центрів сертифікації ключів** (**ЦСК**). Створення та впровадження ЦСК здійснюється згідно правил посиленої сертифікації та вимог НБУ. Результат виконання робіт – створений ЦСК та отримані на нього дозвільні документи, а саме: експертний висновок у галузі КЗІ на програмно-технічний комплекс, атестат відповідності КСЗІ (за необхідності) та свідоцтво про акредитацію чи реєстрацію.

Замовники компанії

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Найбільшими замовниками компанії є:

- Міністерство доходів і зборів України;
- Міністерство внутрішніх справ України;
- Міністерство оборони України;
- Укрзалізниця (Державна адміністрація залізничного транспорту України);
- Міністерство юстиції України;
- Міністерство освіти України;
- НАК “Нафтогаз України”;
- ПАТ “Укрсоцбанк”, АТ “УкрСиббанк”, АТ “Банк “Фінанси та кредит”, ПАТ “інфраструктура відкритих ключів” та інші **банківські, державні і комерційні структури**.

Система електронного цифрового підпису (ЕЦП)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Система ЕЦП (інфраструктура відкритих ключів) – організаційно-технічна **система**, яка інтегрує **сертифікати** відкритих ключів, **засоби ЕЦП** (криптографічних перетворень), **центри сертифікації ключів** (**ЦСК**) та **власників** сертифікатів в **єдину** структуру.

Основними двома елементами системи ЕЦП є **ЦСК** та їх користувачі. **Система ЕЦП** являє собою сукупність взаємодіючих між собою **ЦСК** та кінцевих **користувачів**.

Центри сертифікації ключів (ЦСК)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЦСК державних органів:

► Центральний засвідчувальний орган;

► Державної фіскальної служби України (акредитований);

► Міністерства внутрішніх справ України (акредитований);

► Міністерство оборони України (Збройних сил України - акредитований);

► Міністерства юстиції України (органів юстиції – акредитований);

► ДП “Українські спеціальні системи” (акредитований);

► Державна адміністрація залізничного транспорту України (Укрзалізниця – акредитований);

► ДП “Енергоринок” (ринку електричної енергії – акредитований).

ЦСК банків:

► АТ “УкрСиббанк” (акредитований);

► ПАТ КБ “Приватбанк” (акредитований);

► ПАТ “Укрсоцбанк”, ПАТ “Правексбанк”, ПАТ “ОТП Банк” і ін.

Комерційні ЦСК компаній:

► ТОВ “Ключові системи” (акредитований);

► ТОВ “Арт-мастер” (акредитований) і ін.

Центр сертифікації ключів (ЦСК)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЦСК призначений для **обслуговування** сертифікатів та надання інших **послуг** (**ЕЦП, фіксування часу** та ін.).

ЦСК забезпечує:

► обслуговування **сертифікатів відкритих ключів користувачів, що включає:**

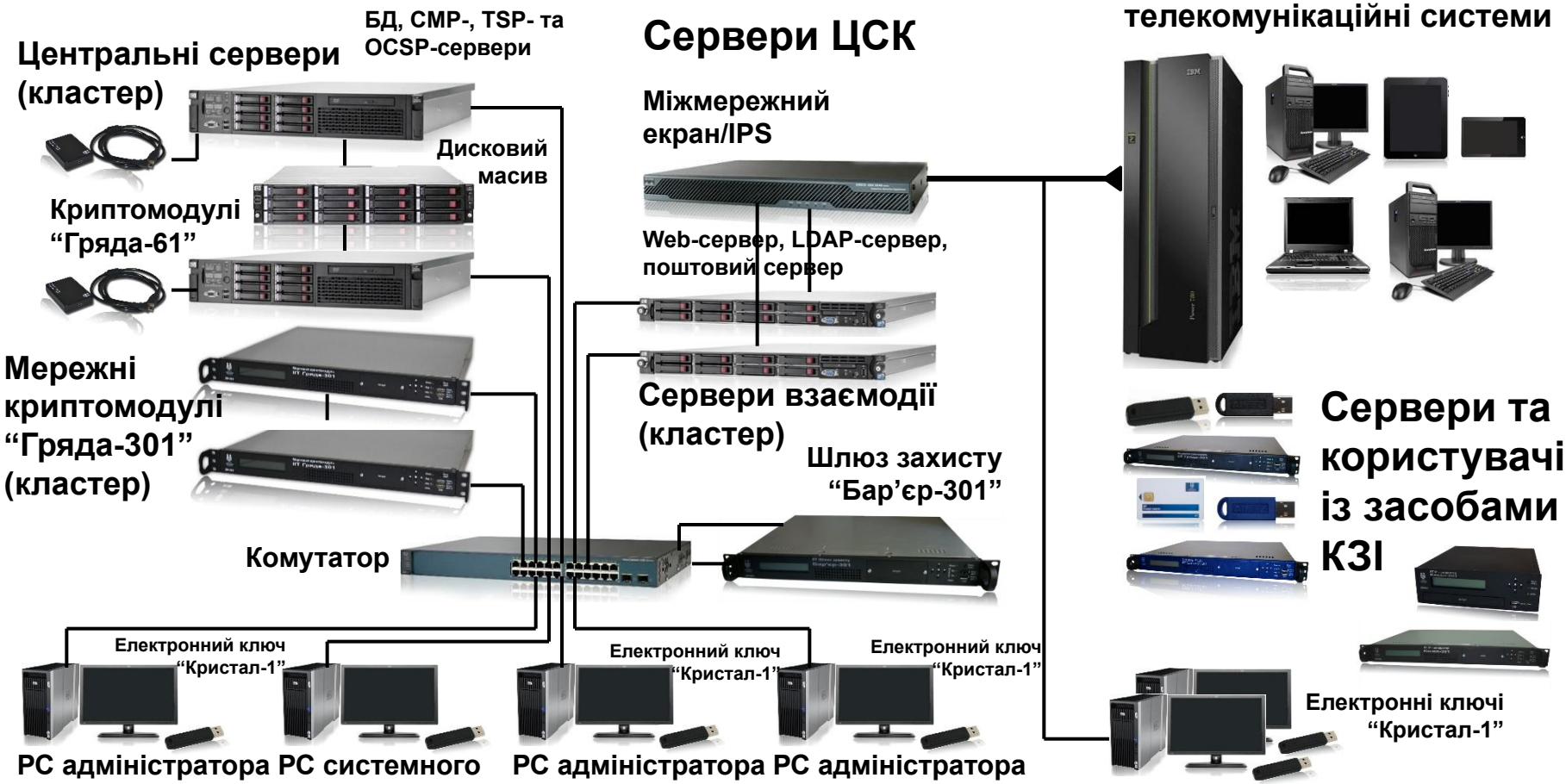
- **реєстрацію** користувачів**;**
- **сертифікацію** відкритих ключів користувачів**;**
- **розповсюдження сертифікатів;**
- **управління статусом** сертифікатів та **розповсюдження** інформації **про статус** сертифікатів**;**

► **надання послуг** фіксування часу**.**

Центр сертифікації ключів (ЦСК)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Програмно-технічний комплекс ЦСК



Робочі місця адміністраторів ЦСК

Засоби центру сертифікації ключів (ЦСК)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

► **Програмний комплекс ЦСК** “ІІТ ЦСК-1” (програмні комплекси центрального сервера, сервера взаємодії, адміністраторів ЦСК та віддаленого адміністратора реєстрації).

► **Апаратні засоби криптографічного захисту інформації (КЗІ)**

І “Гряда-61”

Інтерфейс: USB

Доступ: власний протокол

Швидкодія: 50-100 мс/ЕЦП

Призначення: зберігання та використання особистого ключа ЦСК

мережнии криптомодуль “Гряда-301”

Інтерфейси: 2 x Ethernet 100/1000

Швидкодія: 1200-2000 ЕЦП/с

Призначення: зберігання та використання особистих ключів ЦСК та серверів ЦСК

Електронний ключ “Кристал-1”

Інтерфейс: USB

Призначення: зберігання та використання особистих ключів адміністраторів ЦСК

Криптографічні алгоритми та протоколи

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Шифрування за **ДСТУ ГОСТ 28147:2009, TDEA** та **AES** за ISO/IEC 18033-3.
- ЕЦП за **ДСТУ 4145-2002 та RSA** за PKCS#1 (IETF RFC 3447).
- Гешування за **ГОСТ 34.311-95 та SHA** за ДСТУ ISO/IEC 10118-3:2005.
- Протоколи розподілу ключів за **ДСТУ ISO/IEC 15946-3** (пп. 8.2) та **RSA** за PKCS#1 (IETF RFC 3447).

Формати даних та протоколи взаємодії

► **Сертифікати** та списки відкликаних сертифікатів (**СВС**) згідно вимог до форматів, структури та протоколів, що реалізуються у надійних засобах ЕЦП (державних вимог до надійних засобів ЕЦП) та ISO/IEC 9594-8.
► **Підписані дані** (дані з ЕЦП) згідно державних вимог до надійних засобів ЕЦП та IETF RFC 3161.
► **Захищені дані** (зашифровані дані) згідно вимог до форматів криптографічних повідомлень та IETF RFC 5652.
► Протокол **OCSP** (визначення статусу сертифіката) згідно державних вимог до надійних засобів ЕЦП та IETF RFC 2560.
► Протокол **TSP** (фіксування часу) згідно державних вимог до надійних засобів ЕЦП та IETF RFC 3161.
► Протокол **CMP** (управління сертифікатами).
► Протокол **LDAP** (доступ до LDAP-каталогу).
► **Особисті ключі** згідно PKCS#8 і PKCS#12 та вимог до алгоритмів, форматів і інтерфейсів, що реалізуються у засобах шифрування та надійних засобах ЕЦП.

Носії ключової інформації (НКІ) та криптомодулі

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

► **Електронні диски** (flash-диски).

► **Оптичні компакт-диски** (CD).

► Файлова система (**постійні чи з'ємні диски**).

► **Електронні ключі** "Кристал-1", "Алмаз-1К", Avest AvestKey, Aladdin eToken/JaCarta, Автор SecureToken, Технотрейд uaToken, SafeNet iKey, Giesecke&Devrient StarSign та БІФІТ iBank Key.

► **Смарт-карти** "Карта-1", Техноконсалтинг TEllipse, Aladdin eToken/JaCarta, Автор CryptoCard, Giesecke&Devrient StarSign та БІФІТ Інтегра.

► **Криптомодуль** "Гряда-61" та **мережний криптомодуль** "Гряда-301".

► **Інші носії та криптомодулі** з бібліотеками підтримки, що відповідають вимогам до алгоритмів, форматів і інтерфейсів, що реалізуються у засобах шифрування та надійних засобах ЕЦП з інтерфейсом PKCS#11).

Порядок створення ЦСК

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1 Початкові та передпроектні роботи

► **Категоріювання та обстеження** ЦСК (приміщень та автоматизованої системи).

► Підготовка **початкової організаційно-розпорядчої документації**.

2 Проектні роботи

► Розробка **технічного завдання** на **комплексну систему захисту інформації** (КСЗІ) ЦСК.

► **Погодження технічного завдання** на КСЗІ ЦСК з **Держспецзв'язком України** (за необхідності).

► Розробка вимог до **будівельно-монтажних робіт** у частині **захисту інформації** (за необхідності).

► Розробка **робочого проекту** ЦСК.

► Розробка **експлуатаційної документації** на ЦСК (в т.ч. і **інструкцій з КЗІ**).

► **Погодження інструкцій з КЗІ** з **Держспецзв'язком України** (за необхідності).

► Розробка **організаційно-розпорядчої документації** (в т.ч. і регламенту).

► **Погодження регламенту** з **Держспецзв'язком України** чи іншим вповноваженим органом.

Порядок створення ЦСК

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

3 Створення та впровадження

► Участь у **проведенні будівельно-монтажних робіт** (за необхідності – створення **комплексу ТЗІ** тощо).

► Постачання та монтаж обладнання, інсталяція програмного забезпечення (**розгортання програмно-технічного комплексу**).

► Розробка програми внутрішніх випробувань.

► **Навчання обслуговуючого персоналу**.

► Супровід проведення **внутрішніх випробувань** та проведення **дослідної експлуатації**.

4 Експертизи та акредитація

► Отримання **експертного висновку** на ПТК ЦСК **в галузі КЗІ** Держспецзв'язку України (за необхідністю).

► Підготовка документів до **атестації КСЗІ** в Держспецзв'язку України (організація проведення, за необхідності, експертизи КСЗІ – у галузі ТЗІ).

► Підготовка документів до **акредитації чи реєстрації** у центральному засвідчувальному органі (**ЦЗО**) або засвідчувальному центрі (**ЗЦ**).

► **Супровід** проведення **експертних робіт** під час акредитації чи реєстрації.

Результати створення ЦСК

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Результат виконання робіт – **створений ЦСК** та отримані на нього дозвільні документи:

- **експертний висновок** у галузі **КЗІ** на програмно-технічний комплекс;
- **атестат відповідності КСЗІ** (за необхідності);
- **свідоцтво про акредитацію** чи **посвідчення про реєстрацію**.

Засоби користувача ЦСК (засоби КЗІ)

► **Програмний комплекс користувача ЦСК** “ІІТ Користувач ЦСК-1” (**бібліотеки користувача ЦСК**).

► **Апаратні засоби криптографічного захисту інформації (КЗІ)**

“Гряда-301”

Інтерфейси: 2 x Ethernet 100/1000 (основний та кластерний).

Швидкодія: 1200-2000 ЕЦП/с, 80-500 формувань спільного секрету

“Кристал-1”

Інтерфейс: USB.

Швидкодія: 50-100 мс/ЕЦП

Електронний ключ “Алмаз-1К”

Інтерфейс: USB.

Швидкодія: 150-300 мс/ЕЦП

Смарт-карта “Карта-1”

Інтерфейс: контактний.

Швидкодія: 100-200 мс/ЕЦП

Інтеграція засобів користувача ЦСК (засобів КЗІ)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Бібліотеки користувача ЦСК “ІІТ Користувач ЦСК-1” (засоби криптографічного захисту інформації) інтегруються у прикладні системи через **визначені** інтерфейси (**Microsoft CAPI, PKCS#11, GSS-API, JCA)** і **власні** та реалізовані для **ОС Microsoft Windows** XP/2003 Server/Vista/2008 Server/7/8/2012 Server, Microsoft Windows **CE**/**Mobile** 5/6/6.5, Microsoft Windows **Phone** 7/8, **Linux** (SuSe/Red Hat/Slackware та ін.), **UNIX** (AIX/Solaris/FreeBSD та ін.), **Apple OS X/iOS**, **Google Android** у вигляді бібліотек підключення (DLL/COM, SO, DYLIB – 32/64-біта) або у вигляді архівів **java-класів** для JRE 1.4 та вище (J2ME/J2SE/J2EE).

Для всіх бібліотек користувача ЦСК під всі ОС та платформи, що підтримуються, існують **приклади** їх **використання**.

Комплекс користувача ЦСК

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі

Сервер

ЦСК

Електронний ключ

РС користувача

Особистий ключ

ПК користувача

Захищені електронні дані та документи

Мережний криптомодуль

Особистий ключ

РС користувача

ПК користувача

Забезпечує **автентифікацію користувачів системи на сервері**, **конфіденційність і цілісність даних**, які передаються у системі, а також **цілісність та неспростовність авторства електронних даних і документів**

Інтеграція: офісні пакети, системи електронного документообігу, системи подання звітності, автоматизовані та інтегровані банківські системи тощо

Інтеграція засобів користувача ЦСК (засобів КЗІ)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Бібліотеки користувача ЦСК інтегровані у різні прикладні системи, серед яких:

► **системи електронної пошти** (поштові клієнти та сервери): Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн FossMail та ін.;

► **офісні пакети**: Microsoft Office, Adobe Acrobat та ін.;

► **системи електронного документообігу**: Інфо+ АСКОД, Сітронікс ДокПроф, Софтлайн Мегаполіс, НетКомТехнолоджи Діло та ін.;

► **системи подання звітності** у електронному вигляді до Державної фіскальної служби України, Пенсійного фонду України, Держстату України, МВС України та ін. (компаній 1С, Інтес, НВО Поверхня, Декра і ін.);

► **автоматизовані та інтегровані банківські системи**: SAP for Banking, Oracle FlexCube та ін.;

► **автоматизовані інформаційні системи бюро кредитних історій**;

► більше 80 корпоративних та внутрішньовідомчих систем;

► власні засоби та комплекси криптографічного захисту інформації.

Сервер електронного цифрового підпису (ЕЦП)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інтеграція web-служби: java-модулі (JAX-WS), PL/SQL-модулі, .NET C#-модулі та WWS-модуль. Для інших можливих застосувань надаєтьс WSDL-опис.

Автентифікація клієнтів (серверів): паролі доступу та електронні ключі “Алмаз-1К”.

Захист від НСД: фізичний, виявлення втручань та знищення особистих ключів

Сервер ЕЦП “Блокнот-301”

Інтерфейси: 2 x Ethernet 100/1000 (основний та кластерний).

Доступ: протокол SOAP (web-служба), власний протокол.

Швидкодія: 1700 підписів документів/с, 800 перевірок/с.

Кластеризація: висока доступність та балансування навантаження. Управління: власний графічний інтерфейс.

Моніторинг: власний графічний інтерфейс та сервер моніторингу, протоколи SNMP та syslog

Використання сервера ЕЦП

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сервери прикладних системи

Електронний ключ

Сервери ЕЦП (кластер)

ЦСК

Мережні криптомодулі (кластер)

Швидкодія із балансуванням навантаження: 3500 підписів документів/с

Комплекс захисту електронної пошти

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі (поштові клієнти)

ЦСК

Поштовий сервер

Електронний ключ

РС користувача (поштовий клієнт)

Особистий ключ

ПК користувача (поштовий клієнт)

Захищені поштові повідомленні

Мережний криптомодуль

Особистий ключ

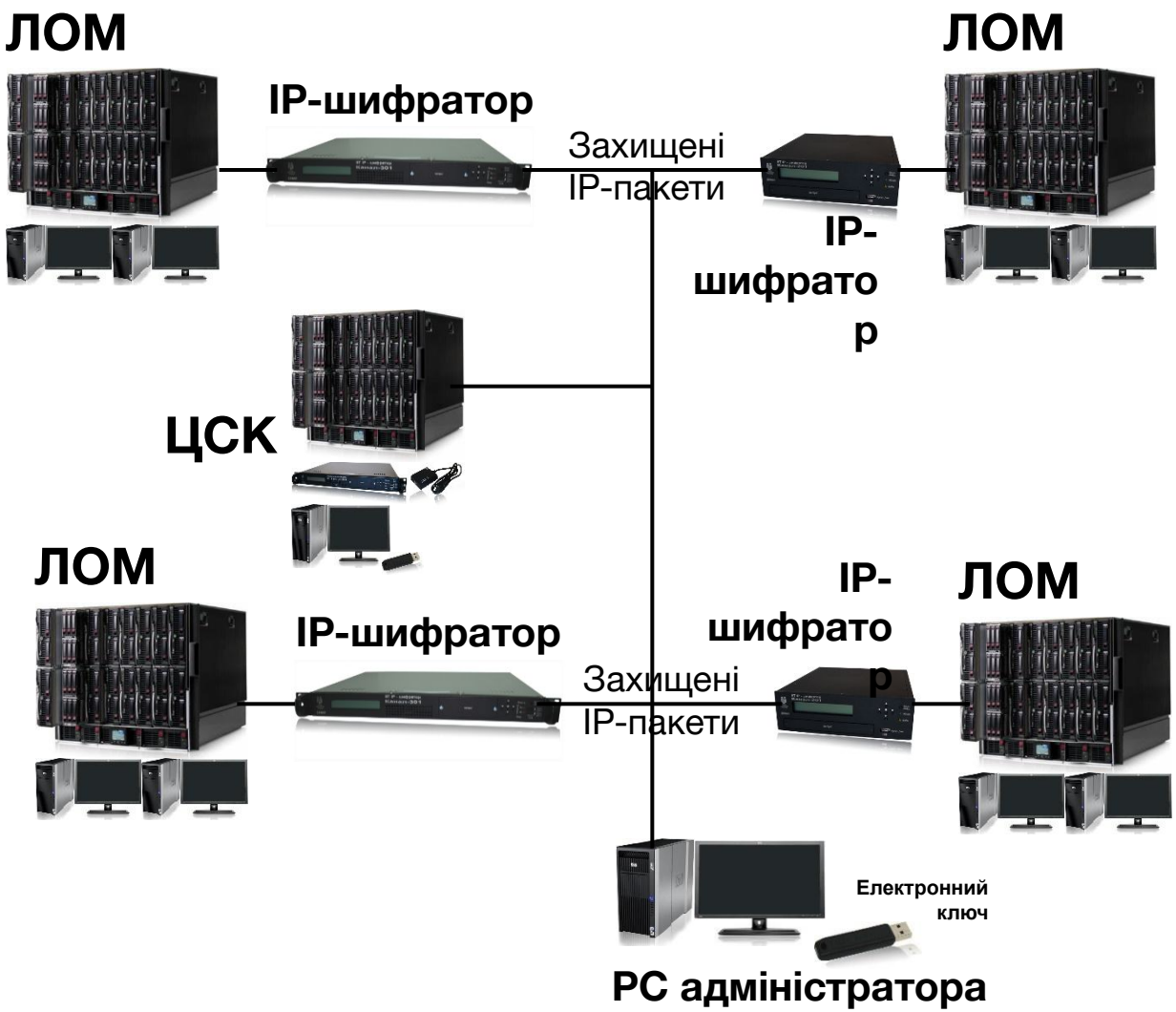
РС користувача (поштовий клієнт)

ПК користувача

Інтеграція: поштові клієнти Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн FossMail

Забезпечує захист (**конфіденційність і цілісність**, а також **цілісність та неспростовність авторства**) **електронних поштових повідомлень** при передачі та зберіганні

Комплекс захисту інформації у IP-мережах

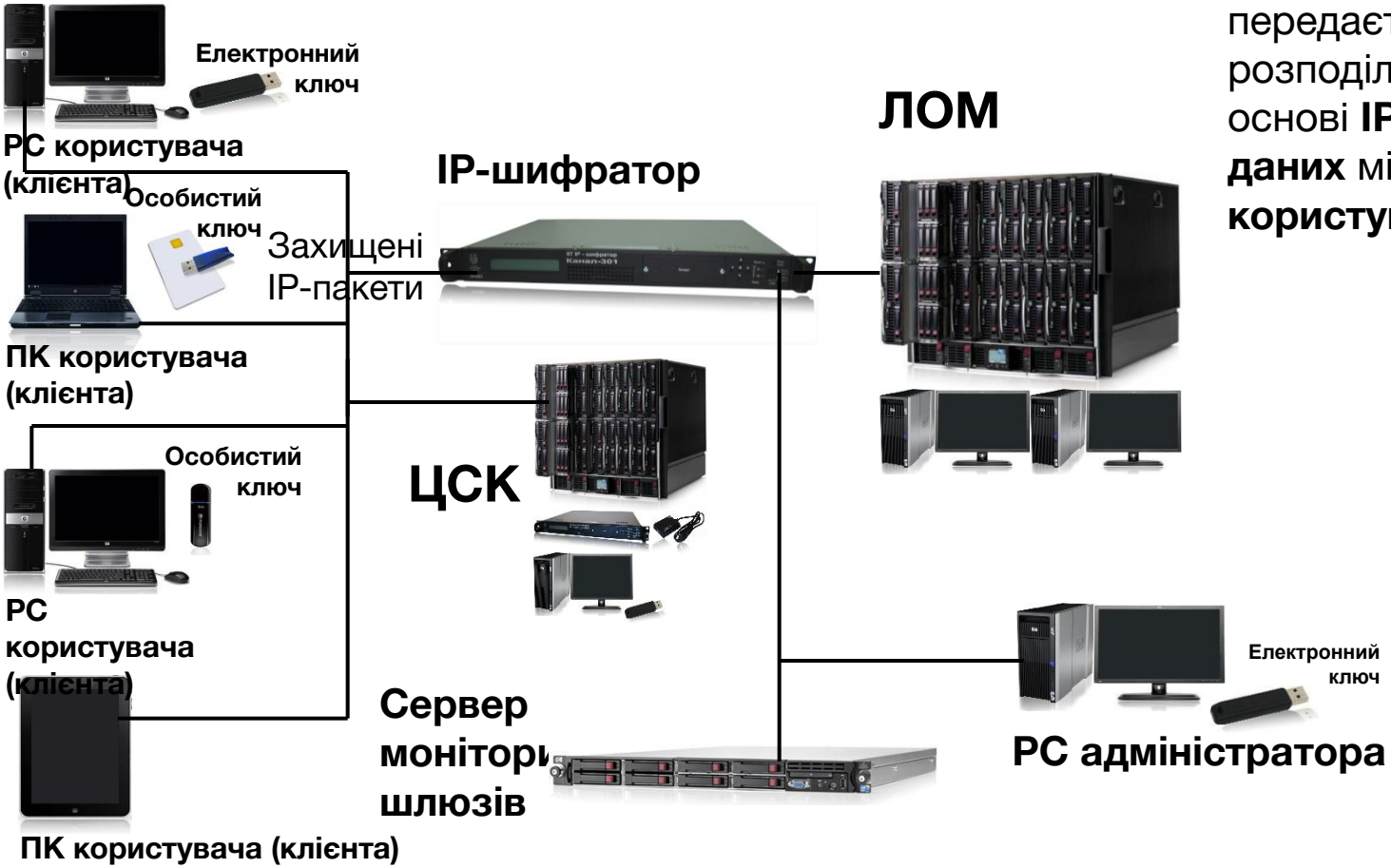


Забезпечує **конфіденційність та цілісність інформації**, яка передається у розподілених системах на основі **IP-мереж передачі даних** між локальними обчислювальними мережами - **ЛОМ**

Комплекс захисту інформації у IP-мережах

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі (клієнти)



Забезпечує **конфіденційність та цілісність інформації**, яка передається у розподілених системах на основі **IP-мереж передачі даних** між **користувачами** та **ЛОМ**

IP-шифратори

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

IP-шифратор “Канал-201” (мікро-пристрій)

Інтерфейси: USB (RNDIS) та Ethernet 10/100

Швидкодія: 25 Мбіт/с

IP-шифратор “Канал-201”

Інтерфейси: 2 x Ethernet 100/1000

Швидкодія: 125 Мбіт/с

IP-шифратор “Канал-301”

Інтерфейси: 2 x Ethernet 100/1000 (RJ-45). Опціонально – 2 x Ethernet 100/1000BASE-SX (оптичні, LC)

Швидкодія: 450 Мбіт/с

Забезпечують шифрування та контроль цілісності потоку IP-пакетів, що передаються через них між ЛОМ та ЛОМ і клієнтами.

Функції:

- **шифрування та контроль цілісності IP-пакетів;**
- **інкапсуляцію IP-пакетів та їх маршрутизацію між мережевими інтерфейсами;**
- **приймання та передачу технологічної (управляючої) інформації;**
- **прийом та введення в дію ключових даних;**
- **встановлення захищених з’єднань з іншими IP-шифраторами та з клієнтами**

Комплекс захисту мережних з’єднань (TCP/IP)

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі (клієнти)

Електронний ключ

РС користувача (клієнта)

Особистий ключ

Захищені TCP-з’єднання

ПК користувача (клієнта)

Особистий ключ

РС користувача (клієнта)

ПК користувача (клієнта)

Шлюзи захисту (кластер)

ЦСК

Сервер моніторингу шлюзів

Сервер

Електронний ключ

РС адміністратора

Забезпечує **автентифікацію клієнтів** (**користувачів**), а також **конфіденційність та цілісність інформації**, яка передається між клієнтськими і серверними частинами прикладних систем (**TCP-з’єднань** між **користувачами** та **сервером**)

Шлюзи захисту з’єднань

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Шлюз захисту “Бар’єр-301” (міні-пристрій)

Інтерфейси: 2 x Ethernet 100/1000.

Швидкодія: 50 автентифікацій/с, 125 Мбіт/с

Шлюз захисту “Бар’єр-301”

Інтерфейси: 2 x Ethernet 100/1000 (RJ-45).

Швидкодія: 100 автентифікацій/с, 250 Мбіт/с

Забезпечують конфіденційність та цілісність інформації, яка передається між клієнтськими і серверними частинами прикладних систем (TCP-з’єднань).

Функції:

- **автентифікація клієнтів та встановлення захищеного TCP-з’єднання;**
- **шифрування даних захищеного TCP-з’єднання;**
- **приймання та передача технологічної (управляючої) інформації;**
- **прийом та введення в дію ключових даних**

Комплекс захисту інформації на носіях

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Забезпечує захист інформації на **носіях інформації** робочих станцій, портативних комп'ютерів та серверів (жорстких дисках, електронних flash-дисках, картах пам'яті тощо).

Захист інформації забезпечується **прозорим шифруванням** областей файлових систем чи створенням віртуальних **логічних** дисків, які фізично є зашифрованими **файлами-образами**.

Засоби захисту носіїв **серверів** підтримують автоматичне **підключення** захищених дисків, аварійне **відключення** та **знищення** захищених дисків, забезпечення доступу до них з ЛОМ та ін.

Засоби захисту носіїв портативних коп'ютерів забезпечують шифрування даних на вбудованих та на зовнішніх картах пам'яті

Комплекс захисту SAP-системи

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі (SAP-клієнти)

Електронний ключ

РС користувача (SAP-клієнт)

ЦСК

Сервер (SAP-сервер)

R/3 Enterprise

Мережні криптомодулі (кластер)

Сервер моніторингу

Особистий ключ

ПК користувача (SAP-клієнт – SAP GUI)

Захищені SNC-з'єднання

Особистий ключ

РС користувача (SAP-клієнт)

ПК користувача (SAP-клієнт)

Забезпечує **автентифікацію користувачів SAP-системи**, **конфіденційність і цілісність даних**, які передаються у системі, а також **цілісність та неспростовність авторства електронних даних і документів**

Інтеграція: SSF-бібліотека, ABAP-модулі, доступ – протокол SSF RFC

Засоби ЕЦП для платформи Oracle FlexCube

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Користувачі (FlexCube-клієнти)

Електронний ключ

РС користувача (клієнта)

Електронний ключ

ПК користувача (клієнта)

Особистий ключ

РС користувача (клієнта)

ПК користувача (клієнта)

ЦСК

Сервери системи (FlexCube-сервер)

Сервери ЕЦП (кластер)

Мережні криптомодулі “Гряда-301” (кластер)

Сервер

FlexCube-клієнти: web-оглядач. Інтеграція: Active-X-бібліотека

FlexCube-сервер: Oracle FlexCube. Інтеграція: web-служба, java-модулі (JAX-WS), PL/SQL-модулі, доступ – протокол SOAP

Забезпечують **цілісність та неспростовність авторства електронних даних і документів**

Засоби захисту входу в контролер домену на базі Microsoft Active Directory

ОС робочої станції (ПК) користувача - Microsoft Windows XP/Vista/7/8/8.1/10.

ОС контролера домену (сервера) - Microsoft Windows Server 2003/2008/2012

Забезпечують **автентифікацію користувачів операційних систем** (**ОС**) **Microsoft Windows** в **контролері домену** на базі **Microsoft Active Directory**.

Обслуговування сертифікатів користувачів та контролера домену здійснює **ЦСК**

Експертні висновки на засоби криптографічного захисту інформації

АТ "Інститут інформаційних технологій"

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Комплекси та засоби криптографічного захисту інформації

Адреса: м. Харків, вул. Бакуліна, 12
Тел./факс: (057) 714-22-05
Web-сайт: iit.com.ua
E-mail: iit@iit.kharkov.ua