

ЗАТВЕРДЖЕНО

Наказ УДЦР

26.05.2017 № 325

(у редакції наказу УДЦР

від 11.11.2022 № 176)

Типове організаційно-технічне рішення з підключення інформаційно-телекомунікаційних систем та робочих станцій операторів телекомунікацій, державних органів та інших суб'єктів господарювання до АІС ЦБД ПН

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ	3
2 НОРМАТИВНІ ПОСИЛАННЯ	4
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ	5
4 ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ.....	6
5 ОСНОВНІ ПОЛОЖЕННЯ	7
6 ВИМОГИ ДО ОРГАНІЗАЦІЇ ЗАХИЩЕНИХ КАНАЛІВ ЗВ'ЯЗКУ	8
7 ВИМОГИ ДО ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПИСУ	10
8 ВИМОГИ ДО ІТС	11
9 ВИМОГИ ДО РС	12
10 ВИМОГИ ДО ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ПРИ ОБМІНІ ЗАЯВКАМИ	13
11 СТИСЛИЙ ОПИС ПРОЦЕСУ ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ДАНИХ	14

1 СФЕРА ЗАСТОСУВАННЯ

У цьому документі наведені організаційно-технічні рішення з підключення інформаційно-комунікаційних систем та робочих станцій операторів телекомунікацій, державних органів та інших суб'єктів господарювання до автоматизованої інформаційної системи «Централізована база даних перенесених номерів» (далі – АІС ЦБД ПН).

В документ можуть бути внесені зміни Адміністратором АІС ЦБД ПН.

2 НОРМАТИВНІ ПОСИЛАННЯ

Цей документ розроблено на виконання:

Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.06 р. № 373;

Порядку надання послуг із перенесення абонентських номерів, затвердженого Рішенням НКРЗІ від 31.07.2015 № 394, зареєстрованого в Міністерстві юстиції України 21.08.2015 за № 1019/27464;

Технічних вимог до телекомунікаційних мереж загального користування України щодо забезпечення надання телекомунікаційної послуги перенесення абонентського номера, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.06.2015 № 355, зареєстрованих в Міністерстві юстиції України 17.07.2015 р. за № 872/27317;

Звіту про науково-дослідну роботу Техніко-економічне обґрунтування впровадження централізованої бази даних перенесених абонентських номерів для реалізації послуг перенесення абонентського номера в Україні, розробник Приватне акціонерне товариство «Український інститут із проектування і розвитку інформаційно-комунікаційної інфраструктури «Діпрозв'язок» (ПрАТ «Діпрозв'язок»);

Рішення НКРЗІ від 25.11.2014 № 777 Про визначення державного підприємства «Український державний центр радіочастот» організацією, яка здійснює централізоване технічне адміністрування персональних номерів та перенесених абонентських номерів;

Технічного завдання на проектування, розроблення та впровадження Автоматизованої інформаційної системи «Централізована база даних перенесених номерів»;

Технічного завдання на створення комплексної системи захисту інформації в інформаційно-комунікаційній системі автоматизована інформаційна система Централізована база даних перенесених номерів, погодженого Державною службою спеціального зв'язку та захисту інформації України.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У даному документі використовуються терміни та визначення згідно з:

ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

4 ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

АІС ЦБД ПН	Автоматизована інформаційно-комунікаційна система «Централізована база даних перенесених номерів»
КНЕДП або АЦСК	Кваліфікований надавач електронних довірчих послуг
ЕП	Електронний підпис
ІТС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
ППН	Процес перенесення абонентських номерів
РС	Робоча станція
ІР VPN	Віртуальна приватна мережа

5 ОСНОВНІ ПОЛОЖЕННЯ

АІС ЦБД ПН призначена для автоматизації процесів:

- перенесення абонентських номерів (далі – ППН) між операторами телекомунікацій;
- інформаційного обміну між операторами телекомунікацій під час ППН;
- збору та обробки інформації про стан ППН, а також про перенесені абонентські номери та їх номери маршрутування.

Послуги із перенесення абонентських номерів реалізуються у взаємодії АІС ЦБД ПН з ІТС та РС операторів телекомунікацій.

ІТС та РС державних органів та суб'єктів господарювання можуть взаємодіяти з АІС ЦБД ПН для отримання інформації про перенесені абонентські номери та її використання у власних технологічних процесах.

Взаємодія АІС ЦБД ПН з ІТС та РС повинна здійснюватися відповідно до закону України «Про захист інформації в інформаційно-комунікаційних системах», а також Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373.

Передача інформації під час взаємодії АІС ЦБД ПН з ІТС та РС операторів телекомунікацій, державних органів та інших суб'єктів господарювання повинна здійснюватися захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Підключення ІТС та РС до АІС ЦБД ПН повинно здійснюватися за одним з двох варіантів наведених на рисунках 1 та 2.

Схема на рис. 1 застосовується при взаємодії АІС ЦБД ПН з ІТС та РС операторів телекомунікацій.

Схема на рис. 2 застосовується при взаємодії АІС ЦБД ПН з ІТС та РС державних органів та інших суб'єктів господарювання (крім операторів телекомунікацій).

6 ВИМОГИ ДО ОРГАНІЗАЦІЇ ЗАХИЩЕНИХ КАНАЛІВ ЗВ'ЯЗКУ

Взаємодія ІТС та РС операторів телекомунікацій з АІС ЦБД ПН на прикладному рівні здійснюється за протоколами WEB (HTTPS), SOAP/XML та SFTP (SSH+FTP).

Взаємодія ІТС та РС державних органів та інших суб'єктів господарювання з АІС ЦБД ПН на прикладному рівні відбувається за протоколами WEB (HTTPS) та SFTP (SSH+FTP).

Взаємодія з використанням зазначених протоколів забезпечується сервером додатків АІС ЦБД ПН. Сервер додатків АІС ЦБД ПН знаходиться в захищеному сегменті локальної обчислювальної мережі АІС ЦБД ПН. Прямий доступ до сервера додатків з боку мережі ІНТЕРНЕТ унеможливлений. Для підключення до сервера додатків АІС ЦБД ПН необхідно організувати захищений канал зв'язку з використанням Комплексу програмного криптографічного захисту інформації «Криптосервер 2.0».

Операторам телекомунікацій, державним органам та іншим суб'єктам господарювання необхідно використовувати «Серверний модуль» зі складу Комплексу програмного криптографічного захисту інформації «Криптосервер 2.0» (далі – КЗІ «Шлюз»), що має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.

Взаємодія засобів КЗІ «Шлюз», встановлених у операторів телекомунікацій, державних органів та інших суб'єктів господарювання, із засобами КЗІ «Шлюз» основного та резервного центрів обробки даних (ОЦОД, РЦОД) АІС ЦБД ПН здійснюється за схемою «Шлюз – Шлюз».

Взаємодія державних органів та інших суб'єктів господарювання (крім операторів телекомунікацій) з АІС ЦБД ПН може здійснюватися також з використанням «Клієнтського модуля» зі складу Комплексу програмного криптографічного захисту інформації «Криптосервер 2.0» (далі – КЗІ «Клієнт»), що має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації (КЗІ «Клієнт» встановлюється на РС). Взаємодія засобів КЗІ «Клієнт», встановлених на РС, із засобами КЗІ «Шлюз» ОЦОД та РЦОД АІС ЦБД ПН, здійснюється за схемою «Клієнт – Шлюз».

Налаштування засобів КЗІ повинно здійснюватися згідно з вимогами експлуатаційної документації на Комплекс програмний криптографічного захисту інформації «Криптосервер 2.0». Налаштування засобів КЗІ «Шлюз» повинно передбачати наявність двох ІР VPN з'єднань: одного – з ОЦОД, другого – з РЦОД.

Засіб КЗІ «Шлюз» може бути розгорнутий на наступних апаратних платформах:

- на базі серверу Hewlett-Packard ProLiant DL360 Gen 9;

- на базі серверів різних виробників обладнання, за умови підтримки функціонування КЗІ «Шлюз»;

- на базі систем віртуалізації різних виробників таких систем, за умови підтримки функціонування КЗІ «Шлюз».

Пропускна здатність захищеного каналу зв'язку за схемою «Шлюз – Шлюз» при використанні різних апаратних або віртуальних платформ залежать від ресурсів фізичного серверу або виділених апаратних ресурсів під віртуальну машину, яка забезпечує функціонування КЗІ «Шлюз».

Пропускна здатність захищеного каналу зв'язку за схемою «Клієнт – Шлюз» при використанні різних апаратних або віртуальних платформ залежать від ресурсів РС або виділених апаратних ресурсів під віртуальну машину, яка забезпечує функціонування КЗІ «Клієнт».

Ключові дані, необхідні для встановлення захищеного з'єднання між засобами КЗІ надаються Адміністратором ЦБД ПН на підставі заяви суб'єкта господарювання, який має намір здійснити підключення до АІС ЦБД ПН. Завірена підписом уповноваженої особи суб'єкта господарювання заява направляється на поштову адресу УДЦР. Ключові дані генеруються уповноваженим представником Адміністратора ЦБД ПН за бажанням у присутності представника оператора телекомунікацій або суб'єкта господарювання та передаються їм на оптичному носії (CD-диск), у подальшому заміна ключових даних може здійснюватися віддалено із використанням встановленого захищеного з'єднання між засобами КЗІ.

7 ВИМОГИ ДО ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПИСУ

Для шифрування персональних даних, які містяться в повідомленнях, якими обмінюються ІТС, РС операторів телекомунікацій та АІС ЦБД ПН під час перенесення абонентського номеру, а також для засвідчення цих повідомлень електронним підписом (далі – ЕП), повинен використовуватися програмний засіб КЗІ «Криптос Гейт Плас» виробництва ТОВ «Ілайф», який має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.

На РС операторів телекомунікацій повинен встановлюватися програмний засіб КЗІ «Криптос Гейт Плас».

В ІТС операторів телекомунікацій повинен бути забезпечений механізм шифрування даних та засвідчення повідомлень електронним підписом за допомогою бібліотек КЗІ «Криптос Гейт Плас».

Для отримання від АЦСК сертифікатів відкритих ключів для ЕП та шифрування, оператор телекомунікацій повинен направити до АЦСК у встановленому АЦСК порядку (відповідно до його регламенту) запит на сертифікацію відкритих ключів. Після надходження запиту АЦСК формує сертифікат відкритого ключа ЕП та шифрування, який має бути переданий іншим операторам телекомунікацій та Адміністратору АІС ЦБД ПН.

8 ВИМОГИ ДО ІТС

В ІТС операторів телекомунікацій повинен бути реалізований веб-сервіс відповідно до специфікації SOAP/XML інтерфейсу взаємодії з АІС ЦБД ПН. Перед підключенням ІТС операторів телекомунікацій до продуктивного середовища АІС ЦБД ПН повинні бути проведені випробування у тестовому середовищі та перевірена коректність реалізації веб-сервісу, шифрування та накладання ЕП.

Параметри для підключення ІТС операторів телекомунікацій до АІС ЦБД ПН надсилаються Адміністратором АІС ЦБД ПН на електронну адресу вказану в заяві на підключення до АІС ЦБД ПН.

За результатом проведення приймальних випробувань підключення ІТС до АІС ЦБД ПН оформляються два примірники відповідного акту. Один примірник акту надається суб'єкту господарювання.

9 ВИМОГИ ДО РС

Параметри для підключення РС до АІС ЦБД ПН через інтерфейси WEB та SFTP надсилаються Адміністратором АІС ЦБД ПН.

Підключення РС державних органів та інших суб'єктів господарювання до АІС ЦБД ПН оформлюється двома примірниками відповідного акту. Один примірник акту надається суб'єкту господарювання.

10 ВИМОГИ ДО ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ПРИ ОБМІНІ ЗАЯВКАМИ

Для захисту персональних даних, що містяться в заявках (повідомленнях спеціалізованого формату у вигляді XML-файлу) на перенесення абонентського номеру, оператор телекомунікацій, який виступає в ролі оператора-отримувача, з використанням уніфікованого прикладного програмного інтерфейсу, а також отриманого від АЦСК посиленого сертифіката відкритого ключа шифрування оператора-донора, здійснює шифрування персональних даних абонентів. Кожен оператор телекомунікацій самостійно здійснює формування особистого та відповідного відкритого ключа шифрування, робить запит на сертифікацію відкритого ключа в АЦСК. Для отримання від АЦСК посиленого сертифіката відкритого ключа шифрування, оператор телекомунікацій повинен передати до АЦСК запит на сертифікацію відкритого ключа у порядку встановленому АЦСК (відповідно до його регламенту). Після надходження відповідного запиту АЦСК формує посилений сертифікат відкритого ключа шифрування.

Прикладне програмне забезпечення ІТС (РС) оператора телекомунікацій повинно забезпечити формування та коректну обробку заявок на перенесення номеру та інших службових повідомлень, обмін якими здійснюється в рамках реалізації ППН. Формат повідомлень визначено в Специфікації SOAP/XML інтерфейсу взаємодії з АІС ЦБД ПН.

11 СТИСЛИЙ ОПИС ПРОЦЕСУ ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ДАНИХ

Оператор-отримувач формує повідомлення з відомостями для перенесення номеру (повідомлення у вигляді XML-файлу). При цьому, в сформованому повідомленні відомості, що містять персональні дані, підлягають шифруванню за допомогою сертифікату відкритого ключа шифрування оператора-донора (направлене шифрування). Інша частина повідомлення залишається в незашифрованому вигляді. Після формування повідомлення оператор-отримувач з використанням власного особистого ключа здійснює підписання повідомлення, шифрування відкритим ключем оператора-донора персональних даних у повідомленні та передачу повідомлення захищеним каналом зв'язку до АІС ЦБД ПН.

Адміністратор АІС ЦБД ПН перевіряє накладений оператором-отримувачем електронний підпис за допомогою сертифікату відкритого ключа шифрування оператора-отримувача (т.з. перевірка авторства повідомлення та його цілісності). Отримане оператором-донором повідомлення розшифровується ним за допомогою власного особистого ключа шифрування.

Директор Департаменту ІТ

Сергій СИРОВЕЦЬ

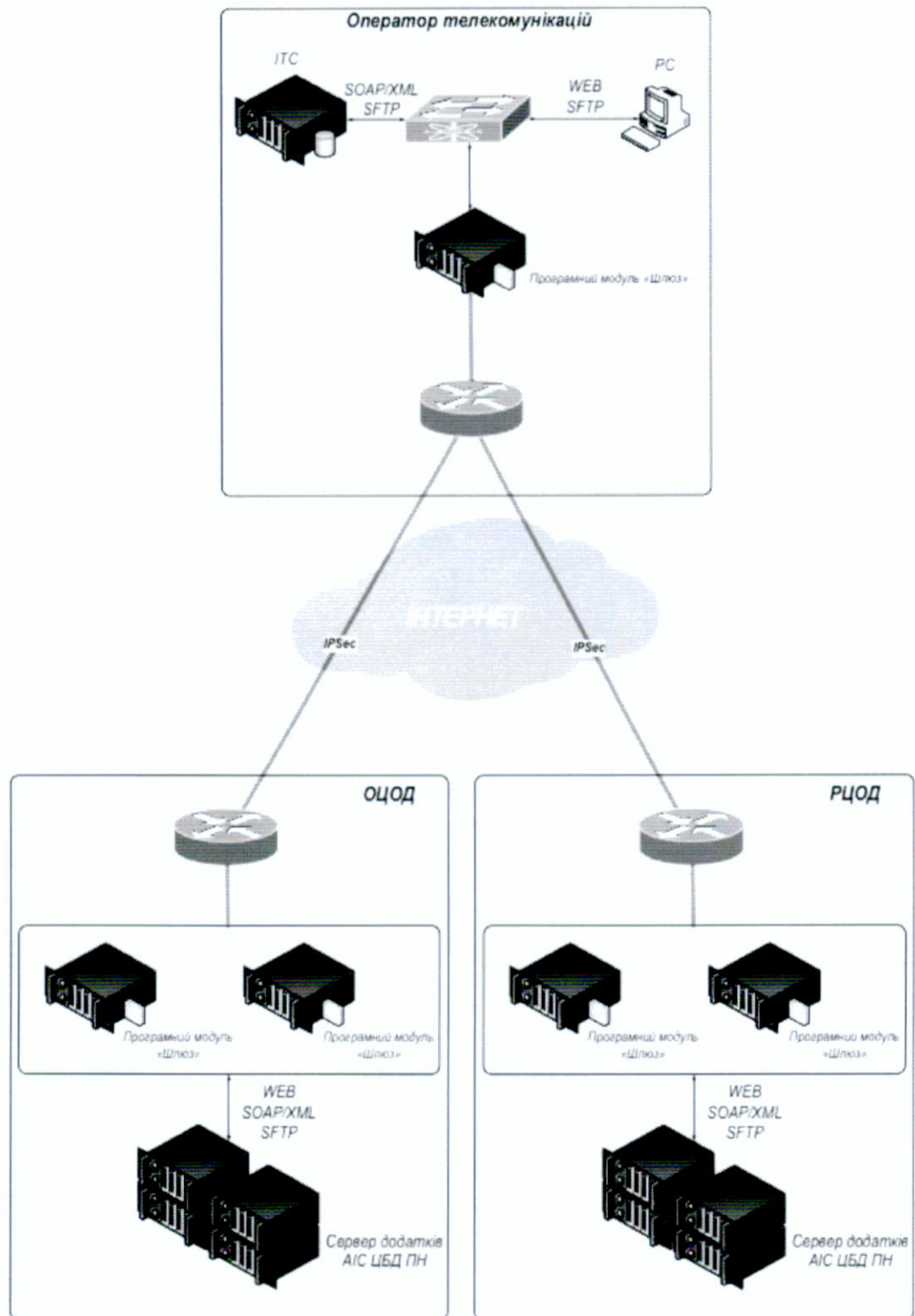


Рисунок 1 – Схема типового підключення ІТС та РС операторів телекомунікацій до АІС ЦБД ПН

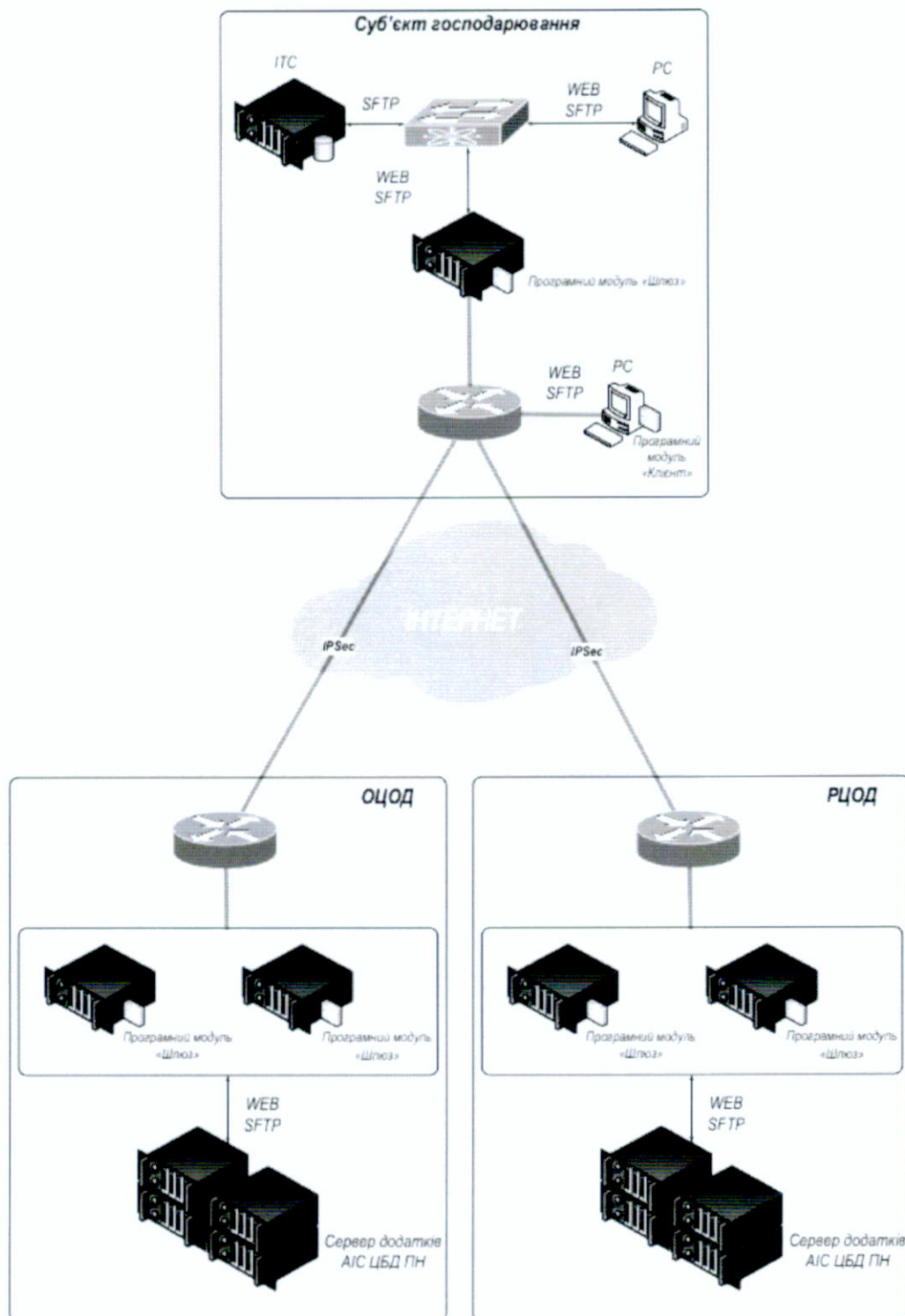


Рисунок 2 – Схема типового підключення ІТС та РС державних органів та інших суб'єктів господарювання до АІС ЦБД ПН