Додаток 1

ЗАТВЕРДЖЕНО
Наказ УДЦР
26.05.2017 № 325

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

На 12 аркушах

Київ 2017

ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ

У цьому документі наведені організаційно-технічні рішення з підключення інформаційно-телекомунікаційних 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-телекомунікаційних системах";

Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.06 р. № 373;

Положення про державну експертизу в сфері технічного захисту інформації, затверджено Адміністрації Державної служби спеціального зв'язку та захисту інформації від 16.05.2007 р. № 93 (зі змінами);

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

Технічних вимог до телекомунікаційних мереж загального користування України щодо забезпечення надання телекомунікаційної послуги перенесення абонентського номера, затверджені наказом Адміністрації Держспецзв'язку від 24.06.2015 № 355, зареєстровані 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 "Про визначення державного підприємства "Український державний центр радіочастот" організацією, яка здійснює централізоване технічне адміністрування персональних номерів та перенесених абонентських номерів" від 25.11.2014 р. № 777;

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

Технічного завдання на створення комплексної системи захисту інформації в автоматизованій інформаційній системі “Централізована база даних перенесених номерів”, узгоджено 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 інформаційна система “Централізована база даних перенесених номерів”
АЦСК	Акредитований центр сертифікації ключів
ЕЦП	Електронний цифровий підпис
ІТС	Інформаційно-телекомунікаційна система
КЗІ	Криптографічний захист інформації
ППН	Процес перенесення абонентських номерів
РС	Робоча станція

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 реалізовуються 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 законів України "Про телекомунікації" та "Про захист інформації в інформаційно-телекомунікаційних системах", а також Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних 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 засобів криптографічного захисту інформації (далі – КЗІ) зі складу програмного комплексу КЗІ "HP - Encryptor UA" виробництва ТОВ "СКЗ "Криптософт".

Операторам телекомунікацій, державним органам та іншим суб'єктам господарювання необхідно використовувати засіб КЗІ "Програмний модуль "Шлюз", що має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації № 05/02/02-595 від 12.02.2015 р.

Взаємодія засобів КЗІ "Програмний модуль "Шлюз", встановлених у операторів телекомунікацій, державних органів та інших суб'єктів господарювання, із засобами КЗІ 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 КЗІ "Програмний модуль "Клієнт" (експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації № 05/02/02-598 від 12.02.2015 р.) зі складу програмного комплексу КЗІ "HP - Encryptor UA", який встановлюється на РС. Взаємодія засобів КЗІ "Програмний модуль "Клієнт", встановлених на РС, із засобами КЗІ ОЦОД та РЦОД АІС ЦБД ПН, здійснюється за схемою "Клієнт – Шлюз".

Налаштування засобів КЗІ повинно здійснюватися згідно з вимогами експлуатаційної документації на програмний комплекс КЗІ "HP - Encryptor UA". Налаштування засобів КЗІ повинно передбачати наявність двох IP VPN-з'єднань: одного – з ОЦОД, другого – з РЦОД.

Засіб КЗІ "Програмний модуль "Шлюз" може бути розгорнутий на наступних апаратних платформах:

- на базі серверів Hewlett-Packard (наприклад, HP ProLiant DL360 Gen 9);
- на базі серверів типу MicroServer Hewlett-Packard (HP ProLiant MicroServer);
- на базі модулів розширення до маршрутизаторів Hewlett-Packard (HP MSR OAP);
- на базі середовищ віртуальних машин серверів Hewlett-Packard.

Пропускна здатність захищеного каналу зв'язку за схемою "Шлюз – Шлюз" при використанні різних апаратних платформ наведена в таблиці:

Засіб КЗІ "Програмний модуль "Шлюз"	**Пропускна здатність у режимі шифрування, Мбіт/с**
На базі серверу HP ProLiant DL360 Gen 9	890 … 900
На базі серверу HP ProLiant MicroServer	55 … 60
На базі модуля розширення	90 … 95

маршрутизатора HP MSR OAP	
На базі середовищ віртуальних машин серверів Hewlett-Packard	Швидкісні параметри залежать від ресурсів фізичного сервера, що виділені під віртуальну машину, яка функціонує в якості Шлюзу

Пропускна здатність захищеного каналу зв'язку за схемою "Клієнт – Шлюз" при використанні різних апаратних платформ становить 45…60 Мбіт/с.

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.

Форму заяви оприлюднено на сайті УДЦР. Завірена підписом уповноваженої особи суб'єкта господарювання заява направляється на поштову адресу УДЦР. Ключові дані направляються Адміністратором АІС ЦБД ПН на електронну адресу, вказану в заяві суб'єкта господарювання.

7 ВИМОГИ ДО ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАКЛАДАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО 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 цифровим підписом (далі – ЕЦП), 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 № 05/02/02-3147 від 27.07.2015 р.

На РС операторів телекомунікацій повинен встановлюватися програмний засіб КЗІ "Криптос Гейт Плас" для операційної системи Microsoft Windows версій 8, 8.1 або 10.

В ІТС операторів телекомунікацій повинен бути забезпечений механізм шифрування даних та засвідчення повідомлень ЕЦП за допомогою бібліотек КЗІ "Криптос Гейт Плас" для середовищ .Net або Java.

Кожен оператор телекомунікацій повинен самостійно сформувати особистий та відповідний йому відкритий ключ шифрування, направити запит на сертифікацію відкритого ключа в Акредитований центр сертифікації ключів

(далі – АЦСК), роботу з яким підтримує програмний засіб КЗІ “Криптос Гейт Плас”.

Для отримання від АЦСК посиленого сертифіката відкритого ключа шифрування, оператор телекомунікацій повинен направити до АЦСК у встановленому АЦСК порядку (відповідно до його регламенту) запит на сертифікацію відкритого ключа. Після надходження запиту АЦСК формує посилений сертифікат відкритого ключа 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 ЕЦП.

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 примірника відповідного акту. Один примірник акту надається суб’єкту господарювання. Форму акту оприлюднено на сайті УДЦР.

9 ВИМОГИ ДО РС

На РС операторів телекомунікацій, державних органів та інших суб’єктів господарювання повинно бути встановлено наступне програмне забезпечення:

- операційна система Microsoft Windows версії 8, 8.1 або 10;
- веб-браузер Internet Explorer 11 або аналогічний;
- програмний засіб КЗІ “Криптос Гейт Плас”.

Параметри для підключення РС до АІС ЦБД ПН через інтерфейси WEB та SFTP надсилаються Адміністратором АІС ЦБД ПН на електронну адресу, вказану в заяві на підключення до АІС ЦБД ПН.

Підключення РС державних органів та інших суб’єктів господарювання до АІС ЦБД ПН оформлюється двома примірниками відповідного акту. Форму

акту оприлюднено на сайті УДЦР. 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 особистого ключа здійснює підписання повідомлення та його передачу захищеним каналом зв'язку до АІС ЦБД ПН.

Адміністратор АІС ЦБД ПН перевіряє накладений оператором-

отримувачем ЕЦП за допомогою сертифікату відкритого ключа шифрування оператора-отримувача (т.з. перевірка авторства повідомлення та його цілісності). При цьому, виконується перевірка статусу сертифіката ключа оператора-отримувача шляхом перевірки його статусу в АЦСК та Центральному засвідчувальному органі або за допомогою протоколів інтерактивного визначення статусу сертифіката (Online Certificate Status Protocol, OCSP) в режимі онлайн. Також виконуються перевірки цілісності ланцюжку сертифікатів, цілісності списків відкликаних сертифікатів, цілісності відповідей за протоколом визначення статусу сертифікатів. Отримане оператором-донором повідомлення розшифровується ним за допомогою власного особистого ключа шифрування.

Центри сертифікації ключів, які надають послуги з генерації ключів та обслуговування сертифікатів відкритих ключів, повинні відповідати наступним вимогам:

– бути акредитованими відповідно до законодавства України;

– забезпечувати відповідність інформаційних об’єктів вимогам спільного наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27.12.2013 р. № 2782/5/689 “Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису”, зареєстрованого в Міністерстві юстиції України 27.12.2013 р. за № 2228/24759.

Директор Департаменту ІТ **А. Кузміч**

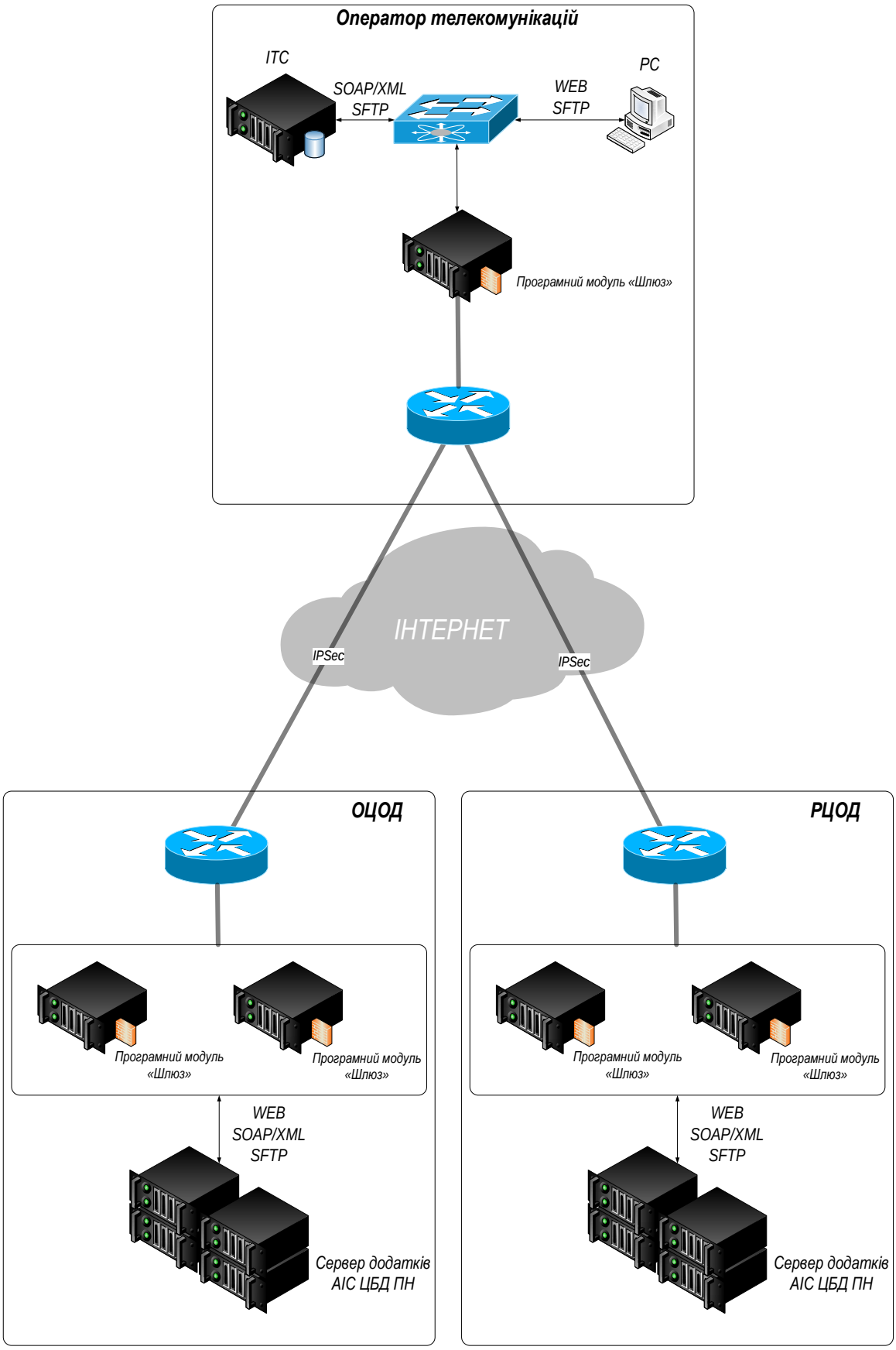

Рисунок 1 – Схема типового підключення ІТС та РС операторів телекомунікацій до АІС ЦБД ПН

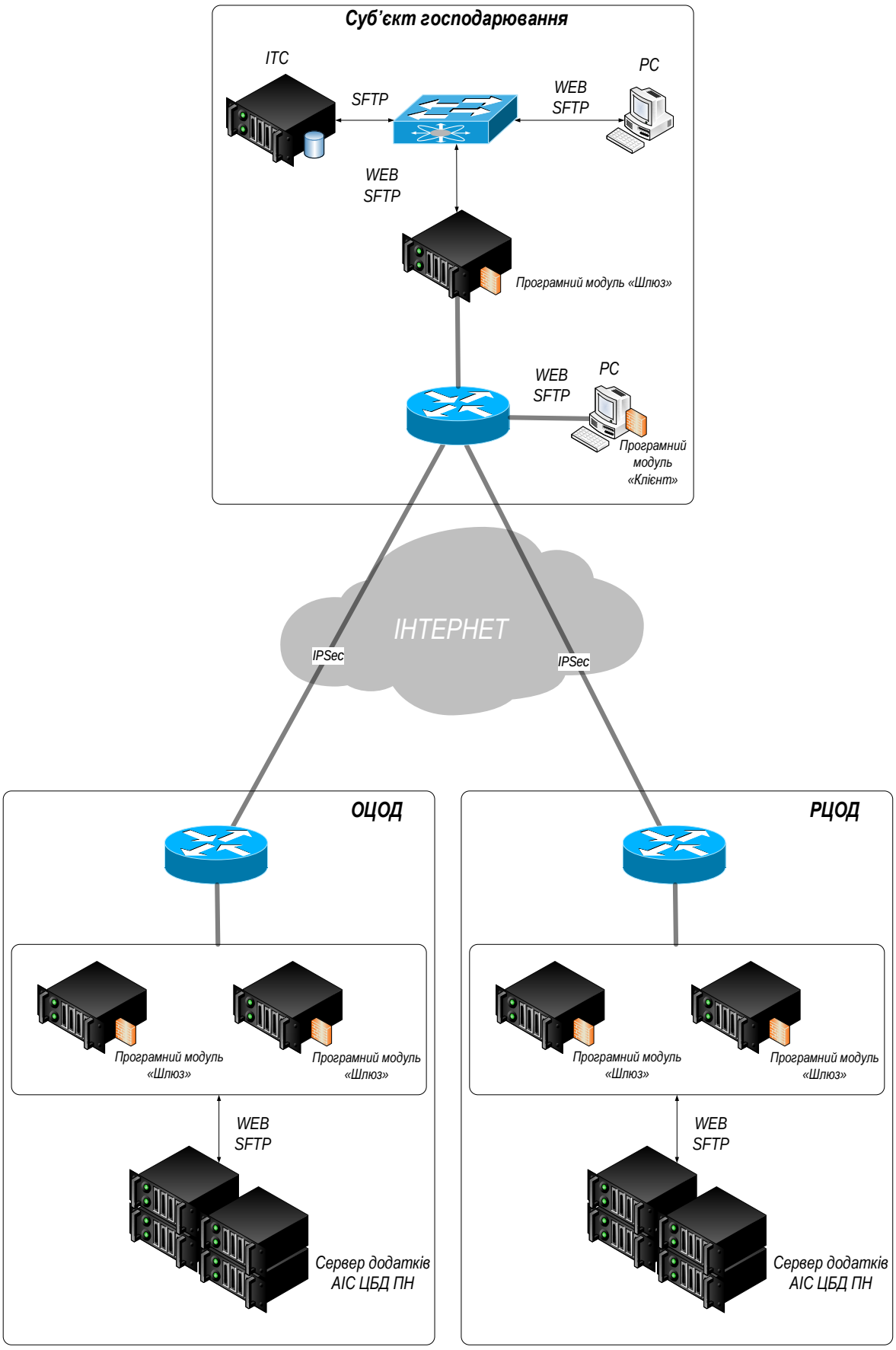

Рисунок 2 – Схема типового підключення ІТС та РС державних органів та інших суб'єктів господарювання до АІС ЦБД ПН