

Додаток 1

ЗАТВЕРДЖЕНО

Наказ УДЦР

06.08.2025 № 169/25

**Вимоги до підключення інформаційно-комунікаційних систем та
робочих станцій операторів електронних комунікацій та інших
суб'єктів господарювання до АІС ЦБД ПН**

Київ 2025

ЗМІСТ

1 ЗАГАЛЬНІ ВІДОМОСТІ.....	3.
2 ТЕРМІНИ ТА СКОРОЧЕННЯ.....	3.
3 НОРМАТИВНІ ПОСИЛАННЯ.....	4.
4 ОСНОВНІ ПОЛОЖЕННЯ.....	5.
5 ВИМОГИ ДО ОРГАНІЗАЦІЇ ЗАХИЩЕНИХ КАНАЛІВ ЗВ'ЯЗКУ.....	6
6 ВИМОГИ ДО ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПISУ.....	9.
7 ВИМОГИ ДО ІКС	9.
8 ВИМОГИ ДО РС	9
9 ВИМОГИ ДО ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ПІД ЧАС ОБМІНУ ПОВІДОМЛЕННЯМИ.....	10.
10 СТИСЛИЙ ОПИС ПРОЦЕСУ ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ДАНИХ	10.

1. ЗАГАЛЬНІ ВІДОМОСТІ

У цьому документі адміністратором централізованої бази даних перенесених номерів визначено вимоги до організації і забезпечення доступу інформаційно-комунікаційних систем та робочих станцій постачальників електронних комунікаційних послуг та суб'єктів господарювання до автоматизованої інформаційної системи «Централізована база даних перенесених номерів».

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

АІС ЦБД ПН	Автоматизована інформаційна система «Централізована база даних перенесених номерів»
Адміністратор АІС ЦБД ПН	УДЦР – організація, яка здійснює функції адміністратора централізованої бази даних перенесених номерів
АЦСК	Акредитований центр сертифікації ключів
ЕП	Електронний підпис
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
ЛБД	Локальна база даних перенесених номерів – копія централізованої бази даних перенесених номерів або її частини, яка розміщена на власних ресурсах постачальника електронних комунікаційних мереж та/або постачальника електронних комунікаційних послуг та використовується в операційних технологічних процесах встановлення з'єднання та/або передачі повідомлення на перенесений номер
Оператор-донор	Постачальник електронних комунікаційних послуг, якому належать індивідуальні права на користування ресурсом нумерації та який надавав електронні комунікаційні послуги за номером з діапазону цього ресурсу нумерації до його перенесення
Оператор-отримувач	Постачальник електронних комунікаційних послуг, якому подано заяву на послугу перенесення номера
ОЦОД	Основний центр обробки даних
ППН	Процес перенесення номера
РС	Робоча станція
РЦОД	Резервний центр обробки даних
ЦБД	Централізована база даних перенесених номерів – єдина база даних, яка призначена для реалізації процесу перенесення номерів, періодичної синхронізації локальних баз даних та зберігання інформації про перенесені номери і їх номери маршрутування
IP VPN	Internet Protocol Virtual Private Network - Віртуальна приватна мережа
SOAP	Simple Object Access Protocol - Протокол обміну структурованими повідомленнями в розподілених обчислювальних системах, базується на форматі XML. SOAP може використовуватися з будь-яким протоколом прикладного рівня: SMTP, FTP, HTTP тощо. Проте, його взаємодія з кожним із цих протоколів має свої особливості, які потрібно відзначити окремо. Найчастіше SOAP використовується разом з HTTP

SFTP Secure File Transfer Protocol – протокол прикладного рівня, призначений для копіювання, передавання та виконання інших операцій з файлами на віддаленому сервері з використанням захищеного з'єднання

Інші терміни та скорочення у цьому документі застосовуються відповідно до: 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».

3. НОРМАТИВНІ ПОСИЛАННЯ

Цей документ розроблено відповідно до:

Закону України «Про захист інформації в інформаційно-комунікаційних системах» (<https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>);

Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373 (із змінами) (<https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>);

Порядку надання послуг перенесення номерів, затверджених постановою Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, від 10.04.2024 № 181, зареєстрованої в Міністерстві юстиції України 28 травня 2024 р. за № 777/42122 (зі змінами);

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, зареєстрованого в Міністерстві юстиції України 17.07.2015 за № 872/27317 (<https://zakon.rada.gov.ua/laws/show/z0872-15#Text>);

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 Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, від 24.07.2024 № 385 «Про визначення державного підприємства «Український державний центр радіочастот» організацією», яка здійснює функції адміністратора централізованої бази даних перенесених номерів» (<https://nkek.gov.ua/npas/risennia-nkek-vid-24072024-no-385-pro-viznacennia-derzavnogo-pidприємства-ukrayinskii-derzavnii-centr-radiocastot-organizacii-i-aka-zdiisniuje-funkcii-administratora-centralizovanoyi-bazi>);

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, погодженого Державною службою спеціального зв'язку та захисту інформації

України, та на підставі зареєстрованого в Адміністрації Державної служби спеціального зв'язку та захисту інформації України атестату відповідності від 07.10.2022 за № 91В на комплексну систему захисту інформації в «Автоматизованій інформаційній системі «Централізована база даних перенесених номерів»».

4. ОСНОВНІ ПОЛОЖЕННЯ

АІС ЦБД ПН призначена для автоматизації процесів:

- перенесення номерів (далі – ППН) між постачальниками електронних комунікаційних послуг (далі – операторами);
- інформаційного обміну між ЛБД (ІКС та РС операторів) та ЦБД з метою забезпечення реалізації процесів перенесення номерів;
- збору та обробки інформації про стан ППН, а також про перенесені номери та їх номери маршрутування.

Послуги перенесення номерів реалізуються шляхом інформаційного обміну відповідними повідомленнями між ЛБД (ІКС та РС операторів) та ЦБД з використанням АІС ЦБД ПН.

ІКС та РС суб'єктів господарювання можуть отримувати доступ до АІС ЦБД ПН для використання даних про перенесені номери в своїх технологічних процесах.

Інформаційний обмін між ЛБД (ІКС та РС) та ЦБД повинен здійснюватися з дотриманням вимог 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 інформаційного обміну між ЛБД (ІКС та РС) операторів і суб'єктів господарювання та ЦБД повинна здійснюватися захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Підключення ІКС та РС до АІС ЦБД ПН повинно здійснюватися за одним з двох варіантів, наведених на рис. 1 та рис. 2.

Схема на рис. 1 застосовується під час інформаційного обміну між АІС ЦБД ПН та ІКС та РС операторів.

Схема на рис. 2 застосовується під час інформаційного обміну між АІС ЦБД ПН та ІКС та РС інших суб'єктів господарювання (крім операторів).

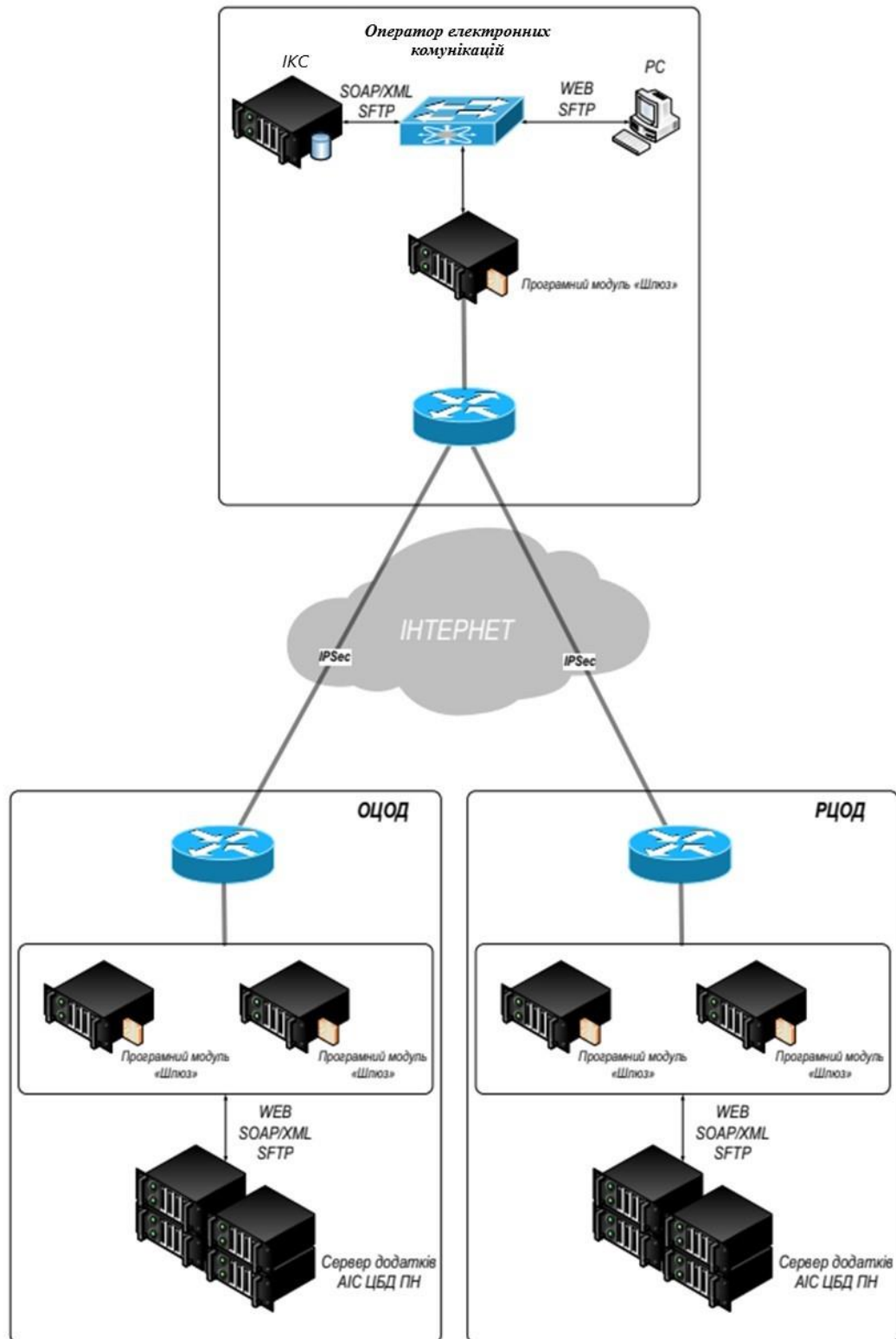


Рис. 1. Схема типового підключення ІКС та РС операторів до АІС ЦБД ПН

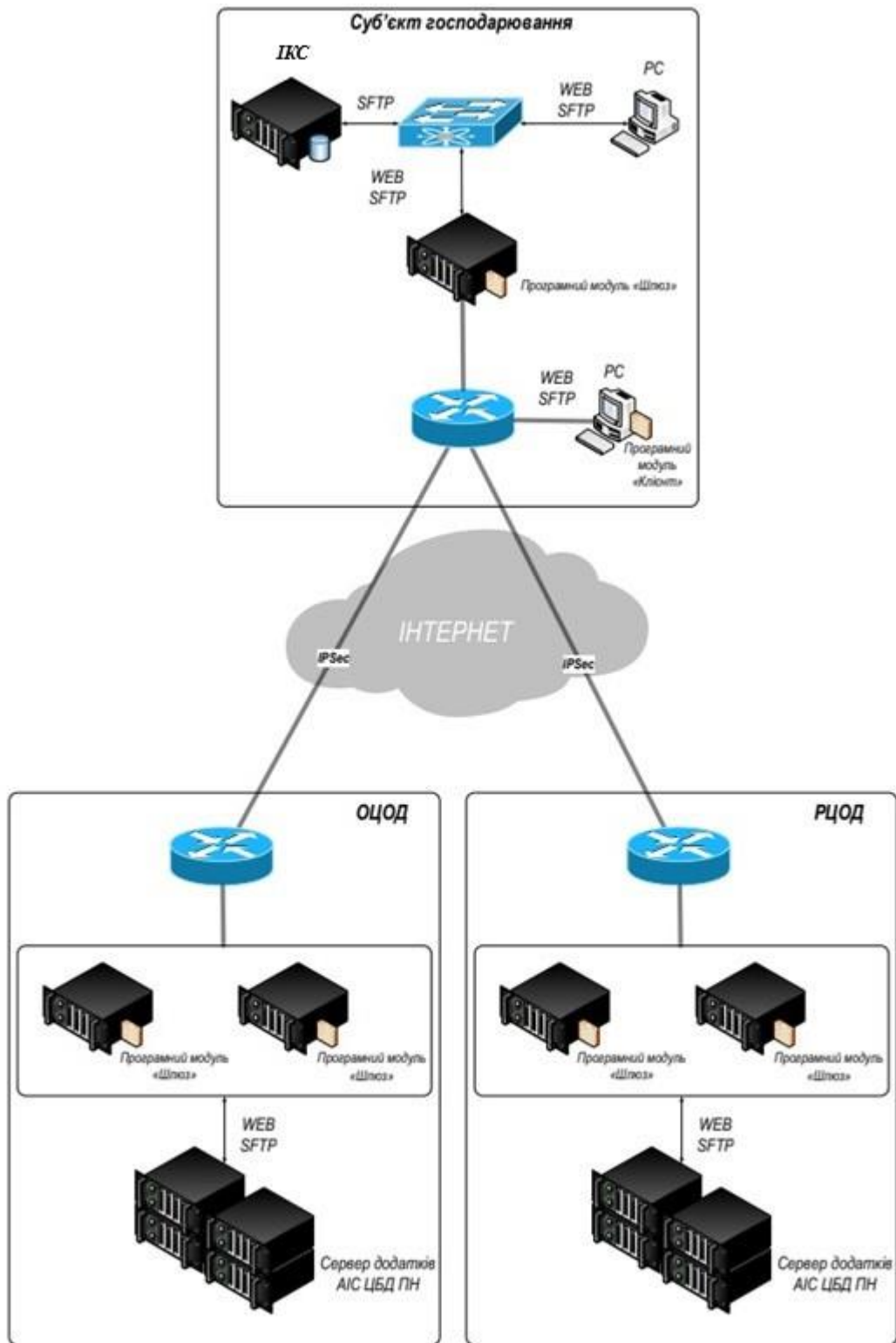


Рис. 2. Схема типового підключення ІКС та РС суб'єктів господарювання до АІС ЦБД ПН

5. ВИМОГИ ДО ОРГАНІЗАЦІЇ ЗАХИЩЕНИХ КАНАЛІВ ЗВ'ЯЗКУ

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

Взаємодія ІКС та РС 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 та 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», установлених в операторів та суб'єктів господарювання, із засобами КЗІ «Шлюз» основного та резервного центрів обробки даних (ОЦОД, РЦОД) АІС ЦБД ПН здійснюється за схемою «Шлюз – Шлюз».

Взаємодія суб'єктів господарювання (крім операторів) 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 IP VPN з'єднань: одного – з ОЦОД, а іншого – з РЦОД.

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

- 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 на підставі заяви суб'єкта господарювання, який отримав дозвіл розпорядника АІС ЦБД ПН на підключення до АІС ЦБД ПН. Завірена підписом уповноваженої особи суб'єкта господарювання заява надсилається на визначену умовами укладеного договору поштову адресу УДЦР. Ключові дані

генеруються уповноваженим представником адміністратора ЦБД представнику/представникам оператора або суб'єкта господарювання та передаються їм на цифровому носії інформації, у подальшому заміна ключових даних може здійснюватися віддалено із використанням встановленого захищеного з'єднання між засобами КЗІ.

6. ВИМОГИ ДО ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПISУ

Для шифрування персональних даних, які містяться в повідомленнях, якими обмінюються ЛБД (ІКС, РС) операторів з використанням АІС ЦБД ПН під час перенесення номера/номерів, 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 повинен встановлюватися програмний засіб КЗІ «Криптос Гейт Плас».

В ІКС операторів 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 повинен надіслати 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 та адміністратору АІС ЦБД ПН.

7. ВИМОГИ ДО ІКС

В ІКС операторів має бути реалізований вебсервіс відповідно до Специфікації SOAP/XML інтерфейсу взаємодії з АІС ЦБД ПН. Перед підключенням ІКС операторів до продуктивного середовища АІС ЦБД ПН повинні бути проведені випробування у тестовому середовищі та перевірена коректність реалізації вебсервісу, шифрування та накладання ЕП.

Параметри для підключення ЛБД (ІКС) операторів до АІС ЦБД ПН надсилаються адміністратором АІС ЦБД ПН на електронну адресу, вказану в заяві на підключення до АІС ЦБД ПН.

За результатом проведених приймальних випробувань щодо підключення ЛБД (ІКС) оператора до АІС ЦБД ПН оформляються два примірники відповідного акту. Один примірник акту надається оператору.

8. ВИМОГИ ДО РС

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 суб'єктів господарювання до АІС ЦБД ПН оформлюється двома примірниками відповідного акту. Один примірник акту надається суб'єкту господарювання.

9. ВИМОГИ ДО ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ПІД ЧАС ОБМІНУ ПОВІДОМЛЕННЯМИ

Для захисту персональних даних, що містяться в заявах (повідомленнях спеціалізованого формату у вигляді XML-файлу) на послугу перенесення номера/номерів, оператор-отримувач 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 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 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 ЛБД (ІКС, РС) оператора повинно забезпечувати формування та коректну обробку заяв на послугу перенесення номера/номерів та інших службових повідомлень, обмін якими здійснюється з використанням АІС ЦБД ПН. Використовується формат повідомлень, визначених у Специфікації SOAP/XML інтерфейсу взаємодії з АІС ЦБД ПН.

10. СТИСЛИЙ ОПИС ПРОЦЕСУ ШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ДАНИХ

Оператор-отримувач формує повідомлення з інформацією про перенесення номера/номерів (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.

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

Директор департаменту ІТ

Сергій СИРОВЕЦЬ