Прим. № 1

ПОГОДЖЕНО
Директор ТОВ "ІНТЕСИС"
_____ О.В. Обухов
"__" _____ 2019 р.

ЗАТВЕРДЖУЮ
Генеральний директор УДЦР
_____ В.І. Корсун
" 08 " 04 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

НА СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ
В АВТОМАТИЗОВАНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ
"ЦЕНТРАЛІЗОВАНА БАЗА ДАНИХ ПЕРЕНЕСЕНИХ НОМЕРІВ"

Шифр "КСЗІ. АІС ЦБД ПН. ТЗ"

ПОГОДЖЕНО
Перший заступник Голови
Державної служби
спеціального зв'язку та захисту
інформації України
_____ О.М. Чаузов
" 12 " 04 2019 р.

2019 рік

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АІС ЦБД ПН	- автоматизована інформаційна система "Централізована база даних перенесених номерів"
ЕОМ	- електронна обчислювальна машина
ІТС	- інформаційно-телекомунікаційна система
КЗЗ	- комплекс засобів захисту
КСЗІ	- комплексна система захисту інформації
НД	- нормативний документ
ОЦОД	- основний центр обробки даних
ППН	- процес перенесення абонентських номерів
РС	- робоча станція
РЦОД	- резервний центр обробки даних
САЗ	- система антивірусного захисту
СЗІ	- служба захисту інформації
СКБД	- система керування базами даних
ТЗ	- технічне завдання
ТЗІ	- технічний захист інформації
ТМЗК	- телекомунікаційна мережа загального користування
ЦБД ПН	- централізована база даних перенесених абонентських номерів

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому технічному завданні (ТЗ) використовуються терміни та визначення згідно з ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99, НД ТЗІ 2.6-001-11 та НД ТЗІ 3.7-003-05.

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Це ТЗ визначає вимоги до створення комплексної системи захисту інформації (КСЗІ) в Автоматизованій інформаційній системі "Централізована база даних перенесених номерів" (далі – АІС ЦБД ПН).

1.1 Повне та умовне найменування комплексної системи захисту інформації, шифр теми

Повне найменування КСЗІ: комплексна система захисту інформації в Автоматизованій інформаційній системі "Централізована база даних перенесених номерів".

Умовне позначення КСЗІ: КСЗІ в АІС ЦБД ПН.

Шифр: КСЗІ. АІС ЦБД ПН. ТЗ.

1.2 Відомості про замовника та виконавця робіт із створення КСЗІ

Замовник: Державне підприємство "Український державний центр радіочастот" (ідентифікаційний код 01181765; місцезнаходження: м. Київ, просп. Перемоги, 151) – Адміністратор АІС ЦБД ПН.

Виконавець: товариство з обмеженою відповідальністю "ІНТЕСИС" (ідентифікаційний код 37356947; місцезнаходження: м. Київ, вул. Преображенська, 23-А).

1.3 Підстави для створення КСЗІ

Підставою для створення КСЗІ в АІС ЦБД ПН є:

– технічне завдання на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів", затверджене 25 січня 2017 р.;

– договір про закупівлю послуг з проектування, розроблення, впровадження та технічної підтримки Автоматизованої інформаційної системи "Централізована база даних перенесених номерів" від 11 січня 2017 р.;

– договір № 317 про надання послуг зі створення комплексної системи захисту інформації в АІС ЦБД ПН від 27 серпня 2018 р. між замовником та виконавцем.

1.4 Відомості про джерела та порядок фінансування робіт

Фінансування робіт зі створення КСЗІ в АІС ЦБД ПН здійснюється за рахунок коштів державного підприємства (ДП) "Український державний центр радіочастот".

1.5 Відомості про терміни початку та закінчення робіт

Терміни початку та закінчення робіт зі створення КСЗІ в АІС ЦБД ПН визначаються згідно з договором № 317 про надання послуг зі створення

комплексної системи захисту інформації в АІС ЦБД ПН від 27 серпня 2018 р. між замовником та виконавцем.

1.6 Порядок оформлення результатів робіт зі створення КСЗІ

Порядок оформлення результатів робіт зі створення КСЗІ в АІС ЦБД ПН повинен відповідати вимогам НД ТЗІ 3.7-003-2005.

1.7 Перелік нормативних документів, що враховуються при створенні КСЗІ

При створенні КСЗІ повинні враховуватися наступні законодавчі, нормативно-правові акти, технічні документи:

– Закон України "Про захист інформації в інформаційно-телекомунікаційних системах";

– Закон України "Про захист персональних даних";

– Указ Президента України від 27 вересня 1999 р. № 1229/99 "Про Положення про технічний захист інформації в Україні";

– Указ Президента України від 22 травня 1998 р. № 505 "Про затвердження Положення про порядок здійснення криптографічного захисту інформації в Україні";

– постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 "Про затвердження Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах";

– Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку України від 16 травня 2007 р. № 93;

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

– НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

– НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

– НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та

комплексних систем захисту інформації в інформаційно-телекомунікаційних системах;

– НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

– ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– Рішення НКРЗІ від 25 листопада 2014 р. № 777 "Про визначення державного підприємства "Український державний центр радіочастот" організацією, яка здійснює централізоване технічне адміністрування персональних номерів та перенесених абонентських номерів";

– Технічні вимоги до телекомунікаційних мереж загального користування України щодо забезпечення надання телекомунікаційної послуги перенесення абонентського номера, затверджені наказом Адміністрації Держспецзв'язку України від 24 червня 2015 р. № 355, зареєстрованим в Міністерстві юстиції України 17 липня 2015 р. за № 872/27317;

– Порядок надання послуг із перенесення абонентських номерів, затверджений Рішенням НКРЗІ від 31 липня 2015 р. № 394, зареєстрованим в Міністерстві юстиції України 21 серпня 2015 р. за № 1019/27464;

– звіт 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"".

Захист інформації та створення КСЗІ в АІС ЦБД ПН повинні здійснюватися на підставі законів України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", а також відповідно до державних стандартів та нормативних документів (НД) у сфері технічного захисту інформації (ТЗІ) в Україні, перелічених вище.

2 ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Мета створення КСЗІ

Метою створення КСЗІ в АІС ЦБД ПН є забезпечення:

– конфіденційності, цілісності та доступності інформації, яка циркулює в АІС ЦБД ПН, від несанкціонованих ознайомлення, модифікації, знищення шляхом здійснення протидії загрозам від дій потенційного порушника;

– забезпечення безпеки інформації, що підлягає захисту, в процесі оброблення її засобами АІС ЦБД ПН, а також під час взаємодії АІС ЦБД ПН з інформаційно-телекомунікаційними системами (ІТС) операторів телекомунікацій, державних органів та суб'єктів господарювання шляхом використання засобів криптографічного захисту інформації.

Захист інформації, що підлягає захисту, повинен забезпечуватися на всіх технологічних етапах обробки інформації і в усіх режимах функціонування АІС ЦБД ПН.

Для забезпечення безпеки інформації, що підлягає захисту, на всіх стадіях життєвого циклу АІС ЦБД ПН КСЗІ передбачається застосування таких заходів та засобів захисту інформації АІС ЦБД ПН:

– організаційні заходи, які реалізуються поза АІС ЦБД ПН;

– технічні заходи, що реалізуються поза АІС ЦБД ПН;

– апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається в АІС ЦБД ПН.

2.2 Призначення КСЗІ

КСЗІ АІС ЦБД ПН призначена для:

– захисту інформації, що підлягає захисту від несанкціонованого доступу;

– керування доступом користувачів до інформаційних ресурсів АІС ЦБД ПН;

– розмежування доступу користувачів АІС ЦБД ПН до інформації, що підлягає захисту;

– блокування несанкціонованих дій, спрямованих на доступ до інформації, що підлягає захисту;

– створення багаторівневого захисту інформаційних ресурсів АІС ЦБД ПН від атак на них;

– контролю та захисту внутрішніх і зовнішніх потоків інформації, яка обробляється розподіленими обчислювальними ресурсами АІС ЦБД ПН;

– реєстрації спроб реалізації загроз інформації та оперативного сповіщення адміністраторів про факти несанкціонованих дій з інформацією, яка підлягає захисту;

– реалізації політики безпеки інформації, прийнятої в АІС ЦБД ПН;

– забезпечення конфіденційності, цілісності та доступності інформації під час експлуатації АІС ЦБД ПН;

– створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного оповіщення адміністраторів про факти несанкціонованого доступу (модифікації, знищення) до інформації, що обробляється та зберігається в АІС ЦБД ПН;

– ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів АІС ЦБД ПН, причин та умов, які спричиняють або можуть привести до порушення її нормального функціонування;

– керування засобами захисту інформації, розмежування доступу користувачів до ресурсів АІС ЦБД ПН, контролю за їх роботою зі сторони осіб, які відповідають за забезпечення безпеки інформації в АІС ЦБД ПН;

– створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування АІС ЦБД ПН;

– організації обліку, зберігання, обігу інформації, яка потребує захисту, та матеріальних носіїв, на яких вона накопичується;

– реєстрації, збору, зберігання, обробки даних про всі події в АІС ЦБД ПН, які мають відношення до безпеки інформації;

– забезпечення доступності ресурсів АІС ЦБД ПН для авторизованих користувачів;

– забезпечення захищеного підключення ІТС операторів телекомунікацій, державних органів та суб'єктів господарювання.

3 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ТА УМОВИ ФУНКЦІОНУВАННЯ

3.1 Функції АІС ЦБД ПН

АІС ЦБД ПН призначена для автоматизації процесів:

– перенесення абонентських номерів (далі – ППН) від оператора-донора до оператора-отримувача;

– інформаційного обміну між операторами телекомунікацій під час ППН;

– збору та обробки інформації про стан ППН, а також перенесені абонентські номери та їх номери маршрутування.

АІС ЦБД ПН забезпечує управління процесами перенесення абонентських номерів між операторами телекомунікацій, а також зберігання інформації про перенесені абонентські номери та їх номери маршрутування на основі централізованої бази даних.

АІС ЦБД ПН є функціонально єдиною системою, базові складові якої утворюють інтегровану інформаційно-комунікаційну інфраструктуру для забезпечення ППН у взаємодії з ІТС операторів телекомунікацій.

3.2 Архітектура АІС ЦБД ПН

Архітектура АІС ЦБД ПН включає наступні складові:

– основний центр обробки даних (ОЦОД);
– резервний центр обробки даних (РЦОД);
– робочі станції (РС);
– робоче місце віддаленого адміністрування.

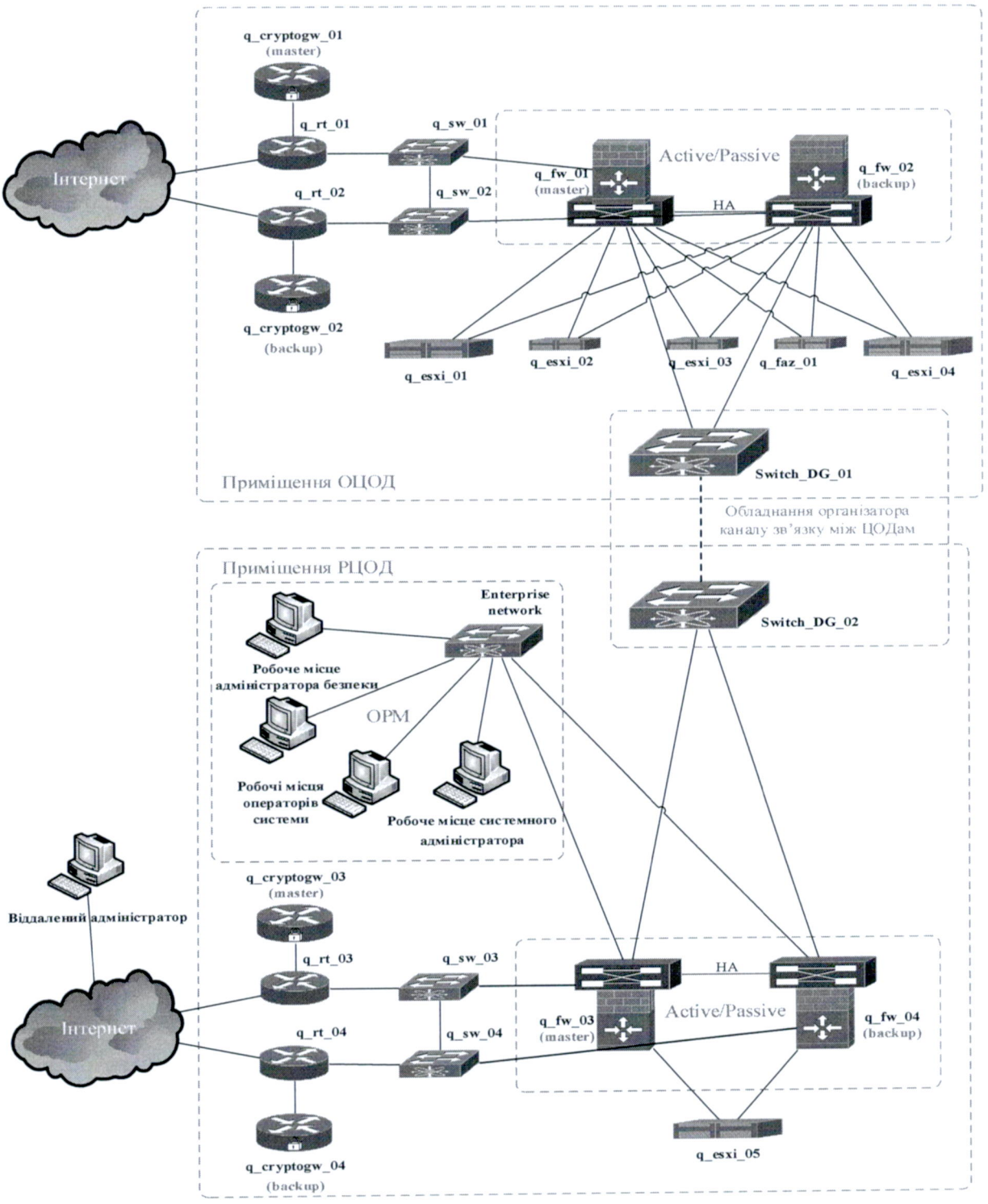
Структурна схема АІС ЦБД ПН наведена на рисунку 3.1, на якій кількість електронних обчислювальних машин (ЕОМ) та технічних засобів телекомунікацій показана умовно.

3.2.1 ОЦОД АІС ЦБД ПН

До складу ОЦОД входять:

– сервери бази даних та додатків – 2 шт.;
– сервери резервного копіювання та тестування – 2 шт.;
– система аналізу журналів та генерування звітів обладнання мережевої безпеки;
– централізована система управління обладнанням мережевої безпеки;
– програмні засоби криптографічного захисту інформації – 2 шт.;
– технічні засоби телекомунікацій (маршрутизатори) – 2 шт.;
– обладнання мережевої безпеки – 2 шт.;
– комутатор – 2 шт.

Остаточний склад ОЦОД визначається на етапі проектування АІС ЦБД ПН.



Умовні позначення

——— Мережа Ethernet 1GBit/s

- - - - - - - - Оптичний канал побудований за технологією DWDM (800 Mbit/s)

Логічні об'єднання

АРМ – обладнання робочих місць

Рисунок 3.1 - Структурна схема АІС ЦБД ПН

3.2.1.1 Сервери баз даних та додатків призначені для:

– забезпечення функціонування прикладного (функціонального) та загального (системного) програмного забезпечення АІС ЦБД ПН;

– розміщення баз даних інформаційних об'єктів, що зберігаються та обробляються в АІС ЦБД ПН;

– забезпечення функціонування системи аналізу журналів та генерування звітів обладнання мережевої безпеки, централізованої системи управління обладнанням мережевої безпеки.

Примітки:

1. Механізми захисту прикладного програмного забезпечення "Автоматизована інформаційна система "Централізована база даних перенесених номерів" повинні пройти оцінювання під час державної експертизи КСЗІ в сфері ТЗІ.

2. Антивірусний захист АІС ЦБД ПН забезпечується на рівні обладнання мережевої безпеки відповідного центру обробки даних (ОЦОД/РЦОД).

3. Остаточні відомості щодо складу програмного забезпечення АІС ЦБД ПН повинні бути визначені та наведені в проектній документації на КСЗІ.

3.2.1.2 Сервери резервного копіювання та тестування призначені для збереження резервних копій програмного забезпечення АІС ЦБД ПН, а також його попереднього налагодження та налаштування.

3.2.1.3 Система аналізу журналів та генерування звітів обладнання мережевої безпеки призначена для збору і аналізу даних з обладнання мережевої безпеки, та забезпечує створення звітів на їх основі, а також надає можливість оцінки вразливості та кореляції подій.

3.2.1.4 Централізована система управління обладнанням мережевої безпеки призначена для управління політиками, оновленнями, ліцензіями обладнання мережевої безпеки, а також управління системою аналізу журналів та генерування звітів з однією консолі.

3.2.1.5 Програмні засоби криптографічного захисту інформації призначені для забезпечення криптографічного захисту інформації, що передається через незахищене середовище.

3.2.1.6 Технічні засоби телекомунікацій призначені для системного поєднання компонентів ОЦОД та РЦОД АІС ЦБД ПН в єдине функціональне середовище.

3.2.1.7 Обладнання мережевої безпеки призначене для забезпечення захисту обладнання, програмного забезпечення та баз даних ОЦОД/РЦОД від інформаційних атак зі сторони телекомунікаційної мережі загального користування (ТМЗК), мережі Інтернет.

3.2.1.8 Обмін інформацією між ОЦОД та РЦОД АІС ЦБД ПН, між АІС ЦБД ПН з ІТС операторів телекомунікацій, державних органів, суб'єктів

господарювання, а також з робочим місцем віддаленого адміністрування здійснюється через мережу Інтернет з використанням засобів криптографічного захисту інформації.

Передача даних між апаратними засобами ОЦОД/РЦОД забезпечується з використанням локальної обчислювальної мережі за стандартом Ethernet.

Передача даних між АІС ЦБД ПН та ІТС операторів телекомунікацій, державних органів, суб'єктів господарювання, а також з робочим місцем віддаленого адміністрування здійснюється зі швидкістю передачі даних, яка забезпечується провайдером послуг мережі Інтернет.

Для інформаційного обміну через мережу Інтернет АІС ЦБД ПН має користуватися послугами захищеного вузла Інтернет доступу провайдерів послуг Інтернет, комплексна система захисту інформації якого має підтверджену відповідністю за результатом державної експертизи в сфері технічного захисту інформації.

3.2.2 РЦОД АІС ЦБД ПН

До складу РЦОД входять:

– сервер бази даних та додатків – 1 шт.;

– програмні засоби криптографічного захисту інформації – не менш ніж 2 шт.;

– технічні засоби телекомунікацій (маршрутизатор) – 2 шт.;

– обладнання мережевої безпеки – 2 шт.;

– комутатор – 2 шт.

Склад апаратних та програмних засобів РЦОД є ідентичним до відповідних апаратних та програмних засобів ОЦОД, остаточний склад яких визначається на етапі проектування АІС ЦБД ПН.

3.2.3 РС АІС ЦБД ПН

РС АІС ЦБД ПН призначені для управління налаштуваннями програмних та апаратних засобів АІС ЦБД ПН, забезпечення доступу користувачів до інформації в базах даних АІС ЦБД ПН відповідно до наданих повноважень, роботи з інформацію, яка зберігається в ЦБД ПН.

На РС АІС ЦБД ПН використовується наступне програмне забезпечення:

– операційні системи Microsoft Windows 8 / 8.1 / 10, комплекси захисту яких мають відповідні експертні висновки в сфері ТЗІ;

– веб-браузер, що забезпечує коректну обробку стандартних html-сторінок;

– антивірусне програмне забезпечення, що має експертний висновок в сфері ТЗІ (визначається на етапі проектування КСЗІ в АІС ЦБД ПН).

3.2.4 Робоче місце віддаленого адміністрування АІС ЦБД ПН

Робоче місце віддаленого адміністрування призначене для забезпечення віддаленого управління налаштуваннями прикладного програмного забезпечення АІС ЦБД ПН.

3.3 Загальна характеристика апаратних та програмних засобів

На серверах АІС ЦБД ПН використовується наступне програмне забезпечення:

– платформа віртуалізації – VMware vSphere 6 Standard;
– операційні системи серверів – Oracle Linux 7, Centos 7;
– система керування базами даних Oracle Database 12;
– прикладне програмне забезпечення "Автоматизована інформаційна система "Централізована база даних перенесених номерів"".

Остаточний перелік програмного забезпечення, що використовується на серверах АІС ЦБД ПН, визначається на етапі проектування АІС ЦБД ПН.

Для розгортання серверів АІС ЦБД ПН використовуються ЕОМ серверного типу HP DL380 Gen9 24SFF CTO Server або аналогічні/кращі за характеристиками. Деталізовані відомості щодо апаратного забезпечення ЕОМ, що входять до складу АІС ЦБД ПН, наведені в формулярі АІС ЦБД ПН.

Для розгортання програмних засобів криптографічного захисту інформації використовується ЕОМ серверного типу HP DL360 Gen9 8SFF CTO Server.

В ОЦОД та РЦОД використовуються маршрутизатори моделі HP MSR 3044 та обладнання мережевої безпеки виробника Fortinet моделі Fortigate 100d/200d, які повинні мати позитивний експертний висновок в сфері ТЗІ.

Електроживлення всіх серверів та технічних засобів телекомунікацій ОЦОД/РЦОД здійснюється від відповідних джерел безперебійного живлення. У разі збою електроживлення, повинно забезпечуватися автоматичне коректне завершення роботи серверів за відповідною налаштованою програмною командою від джерела безперебійного живлення (згідно з вимогами до електроживлення елементів АІС ЦБД ПН).

Для криптографічного захисту інформації, що циркулює в АІС ЦБД ПН, між АІС ЦБД ПН та ІТС операторів телекомунікацій, а також з робочим місцем віддаленого адміністрування, передбачається використання наступних засобів криптографічного захисту інформації:

– для створення захищених каналів зв'язку між складовими елементами АІС ЦБД ПН, між АІС ЦБД ПН та ІТС операторів телекомунікацій, державних органів, суб'єктів господарювання – програмний комплекс криптографічного захисту інформації, який повинен мати позитивний експертний висновок в сфері криптографічного захисту інформації;
– для шифрування інформації в повідомленнях операторів під час перенесення номеру – програмний засіб криптографічного захисту інформації, який повинен мати позитивний експертний висновок в сфері криптографічного захисту інформації.

3.4 Функціональна структура АІС ЦБД ПН

Функціональна структура АІС ЦБД ПН включає наступні компоненти (підсистеми):

– централізована база даних перенесених абонентських номерів (ЦБД ПН);
– підсистема інтерфейсів;
– інформаційно-аналітична підсистема;
– підсистема аудиту та звітності;
– підсистема адміністрування і безпеки;
– підсистема моніторингу;
– підсистема технічної підтримки (HelpDesk);
– підсистема криптографічного захисту інформації.

Функціональна структура АІС ЦБД ПН наведена на рисунку 3.2.

Рисунок 3.2 - Функціональна структура АІС ЦБД ПН

3.4.1 ЦБД ПН

ЦБД ПН забезпечує виконання наступних функцій:

– здійснює збір та обробку даних про перенесені абонентські номери і їх номери маршрутування;
– забезпечує можливість оновлення даних для операторів телекомунікацій про перенесені номери і номери маршрутування в режимі онлайн при завершенні ППН;
– забезпечує можливість для операторів телекомунікацій отримання оновленої інформації про перенесені номери і номери маршрутування в режимі офлайн;
– надає доступ до архівних даних для зберігання і синхронізації в режимі офлайн;
– забезпечує оновлення інформації про перенесені номери в режимі офлайн;

– зберігає дані про Національний план нумерації і дані про приналежність номерів тому або іншому оператору телекомунікацій;

– забезпечує автоматизоване введення актуальних даних Національного плану нумерації.

3.4.2 Підсистема інтерфейсів

Підсистема інтерфейсів забезпечує доступ користувачів АІС ЦБД ПН до сервісів та програмних модулів прикладного програмного забезпечення АІС ЦБД ПН.

Функціонально підсистема інтерфейсів складається з графічного WEB-інтерфейсу користувача, SOAP/XML-інтерфейсу та SFTP-інтерфейсу.

3.4.3 Інформаційно-аналітична підсистема

Інформаційно-аналітична підсистема забезпечує виконання наступних функцій:

– здійснює централізоване автоматичне адміністрування процесів перенесення і повернення абонентського номера мобільного зв'язку;

– здійснює реєстрацію заявок на перенесення номера, що поступають в АІС ЦБД ПН;

– здійснює перевірку первинної інформації, що знаходиться в заявці на перенесення номера;

– здійснює управління процесами перенесення одного номера, декількох номерів або інтервалу номерів в одній заявці з можливістю скасування перенесення одного або декількох номерів, як зі сторони оператора-отримувача, так і зі сторони базового оператора/оператора-донора;

– реєструє всі етапи та строки ППН, контролює дотримання строків перенесення номера згідно з вимогами нормативних документів;

– здійснює підтримку одночасно декількох ППН з можливістю розподілу по учасниках;

– забезпечує дотримання структурності процесу й послідовності повідомлень із зазначенням зв’язків між запитами та відповідями;

– підтверджує в автоматичному режимі кожну отриману заявку із вказівкою на можливі помилки;

– має можливість описувати нові процеси перенесення номера або змінювати існуючі процеси без істотних змін програмного забезпечення й зупинки системи;

– при зміні параметрів процесів здійснює підтримку двох версій одного процесу – старого для заявок, поданих до зміни процесу, та нових, поданих після внесення змін до процесу;

– забезпечує можливість проводити тестування процесів у прискореному режимі для скорочення загального часу тестування;

– забезпечує можливість реалізувати покрокове тестування етапів процесу перенесення номера в автоматичному режимі з фіксацією помилок;

– забезпечує формування звітів щодо даних Національного плану нумерації;

– здійснює адміністрування процесу перенесення географічних та негеографічних номерів;

– забезпечує можливістю повернення номера (номерів) оператору-донору у випадку, коли користувач розірвав контракт із оператором-отримувачем, протягом (не більше) 24 годин після розірвання договору.

3.4.4 Підсистема аудиту та звітності

Підсистема аудиту та звітності виконує такі функції:

– надає можливість отримати інформацію про хід ППН, відхилення від встановлених правил перенесення номера, статистичні звіти про надання ППН;

– має інструменти для забезпечення збору статистичних даних користувачами;

– забезпечує експорт даних у формати MS Excel, MS Word, PDF, CSV, імпорт даних з формату MS Excel.

3.4.5 Підсистема адміністрування і безпеки

Підсистема адміністрування і безпеки забезпечує виконання таких функцій:

– створення нових облікових записів користувачів, наділення їх необхідними правами та ролями, управління цими правами та вилучення облікових записів користувачів;

– забезпечує авторизацію користувачів відповідно до їх прав і повноважень;

– забезпечує ідентифікацію, автентифікацію та управління доступом користувачів.

3.4.6 Підсистема моніторингу

Підсистема моніторингу контролює статус і завантаження інтерфейсів та забезпечує моніторинг:

– функціонування та контролю параметрів АІС ЦБД ПН (рівень завантаження програмних і апаратних компонентів АІС ЦБД ПН; рівень використання ресурсів);

– кількості заявок, що обробляються та знаходяться у черзі на обробку;

– вхідних параметрів заявки на перенесення номера її статус/крок виконання, час початку обробки заявки;

– дотримання якості сервісу на етапах перенесення номера.

3.4.7 Підсистема технічної підтримки

Підсистема технічної підтримки забезпечує:

– можливість операторам телекомунікацій реєструвати повідомлення про проблеми та хід їх усунення;

– можливість керувати процесом усунення проблем, вести журнал усунення проблем, зберігати історію про проблеми та хід їх усунення.

3.4.8 Підсистема криптографічного захисту інформації

Підсистема криптографічного захисту інформації забезпечує реалізацію функцій криптографічного захисту інформації, яка передається каналами передачі даних мережі Інтернет.

Для захисту даних абонентів оператор телекомунікацій, який ініціює перенесення номеру, здійснює шифрування лише даних, які містяться в повідомленні оператора під час ППН, з використанням сертифіката відкритого ключа шифрування оператора, який обслуговує на даний момент номер. В АІС ЦБД ПН відсутня можливість розшифрування даних абонента, що містяться в повідомленнях операторів, обмін якими здійснюється під час ППН. Інша інформація, отримана від операторів телекомунікацій, під час ППН, має оброблюватися в АІС ЦБД ПН.

Завдання генерації та управління ключовими даними, необхідними для виконання зазначених операцій, не входить до завдань прикладного програмного забезпечення АІС ЦБД ПН.

В складі підсистеми криптографічного захисту інформації використовуються засоби криптографічного захисту інформації, які повинні мати позитивні експертні висновки в сфері криптографічного захисту інформації.

3.5 Характеристика інформації, що обробляється в АІС ЦБД ПН

3.5.1 Узагальнені відомості про інформацію, що обробляється та зберігається в АІС ЦБД ПН

Узагальнені відомості про інформацію, що обробляється та зберігається в АІС ЦБД ПН, наведені в таблиці 3.1.

Таблиця 3.1 – Узагальнені відомості про інформацію, що обробляється та зберігається в АІС ЦБД ПН

№ з/п	Вид інформації	Стисла характеристика інформації	Обмеження доступу до інформації	Вигляд даних
1	Програмне забезпечення АІС ЦБД ПН	Операційні системи, прикладне програмне забезпечення, антивірусне програмне забезпечення	Відкрита	У вигляді файлів
2	Журнали реєстрації подій	Журнали реєстрації подій, що ведуться апаратними та програмними засобами АІС ЦБД ПН	Конфіденційна (технологічна)	У вигляді файлів та об'єктів бази даних
3	Файли конфігурації програмного та апаратного забезпечення	Файли конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи АІС ЦБД ПН	Конфіденційна (технологічна)	У вигляді файлів

№ з/п	Вид інформації	Стисла характеристика інформації	Обмеження доступу до інформації	Вигляд даних
4	Інформація, що зберігається в базі даних АІС ЦБД ПН			
4.1	Блок зашифрованих даних в заявці на перенесення номеру	Блок зашифрованих даних в заявці на перенесення номеру, що призначений для передачі даних абонентів від одного оператора іншому без можливості їх розшифрування в АІС ЦБД ПН	Відкрита	У складі xml-файлів спеціалізованого формату в зашифрованому вигляді
4.2	Дані перенесених абонентських номерів	Відомості про перенесені абонентські номери абонентів операторів телекомунікацій	Відкрита	У вигляді об'єктів бази даних
5	Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	Відкрита	У вигляді файлів

В АІС ЦБД ПН циркулюють наступні типи інформації:

1) технологічна інформація (системні налаштування, налаштування безпеки програмного та апаратного забезпечення АІС ЦБД ПН, ідентифікатори користувачів АІС ЦБД ПН та їх облікові записи, журнали реєстрації тощо), наведена в п.п. 1 – 3 таблиці 3.1; технологічна інформація є інформацією з обмеженим доступом, яка доступна тільки адміністраторам АІС ЦБД ПН згідно з їх службовими обов'язками;

2) конфіденційна інформація (технологічна інформація), наведена в таблиці 3.1.

Відомості щодо забезпечення властивостей (конфіденційності, цілісності, доступності та спостережності) інформації, що зберігається та обробляється в АІС ЦБД ПН, наведені в таблиці 3.2.

Таблиця 3.2 – Відомості щодо забезпечення властивостей інформації, що зберігається та обробляється в АІС ЦБД ПН

Вид інформації (згідно з таблицею 3.1)	Відомості щодо забезпечення властивостей інформації			
	конфіденційність	цілісність	доступність	спостережність
Програмне забезпечення ЕОМ	-	+	+	+
Журнали реєстрації подій	+	+	+	+

Вид інформації (згідно з таблицею 3.1)	Відомості щодо забезпечення властивостей інформації			
	конфіденційність	цілісність	доступність	спостережність
Файли конфігурації програмного та апаратного забезпечення	+	+	+	+
Інформація, що зберігається в базах даних	+	+	+	+
Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	+	+	+	+

3.5.2 Забезпечення захисту даних абонентів

Забезпечення захисту даних абонентів відповідних операторів телекомунікацій здійснюється операторами телекомунікації при оформленні заявки на перенесення номеру. В АІС ЦБД ПН дані абонентів циркулюють виключно в зашифрованому вигляді без можливості їх розшифрування відповідно до вимог ТЗ на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів".

3.5.3 Порядок обробки та зберігання інформації в АІС ЦБД ПН

Обробка та зберігання інформації в АІС ЦБД ПН здійснюється у встановленому порядку з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373, та ТЗ на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів".

3.5.4 Стисла характеристика ППН та повернення номера абоненту АІС ЦБД ПН

ППН передбачає наступну послідовність:

1) абонент подає заявку про перенесення номера новому оператору – оператору-отримувачу;

2) оператор-отримувач формує та передає відповідний запит про перенесення номера до АІС ЦБД ПН;

3) АІС ЦБД ПН перевіряє правильність інформації в запиті і пересилає його оператору-донору / базовому оператору. Якщо в запиті про перенесення номера виявлена невірна інформація, то його буде відхилено, а оператору-отримувачу буде відправлено повідомлення про відхилення;

4) оператор-донор / базовий оператор перевіряє правильність інформації в запиті про перенесення номера і повинен надати одну відповідь з трьох можливих варіантів:

– оператор-донор / базовий оператор приймає і підтверджує запит про перенесення номера, надіславши повідомлення, яким підтверджує перенесення номера;

– у разі, якщо отримана в запиті про перенесення номера інформація не пройшла перевірку оператора-донора / базового оператора, оператор-донор / базовий оператор посилає відповідне повідомлення, зазначивши причину відхилення заявки про перенесення номера;

– якщо оператор-донор / базовий оператор не надав відповідь на запит про перенесення номера протягом встановленого періоду часу, то АІС ЦБД ПН автоматично надсилає повідомлення про погодження донора.

У разі, якщо в одній заявці про перенесення номера переноситься декілька номерів, є можливість вилучити декілька номерів з первинного запиту без зупинки процесу і скасування процесу перенесення номера. Вилучення номера може здійснювати як оператор-донор / базовий оператор, так і оператор-отримувач.

Абонент має право скасувати замовлення про перенесення номера доки не підписаний договір з оператором-отримувачем. У разі скасування перенесення номера абонентом, оператор-отримувач посилає повідомлення про скасування перенесення до АІС ЦБД ПН. АІС ЦБД ПН пересилає повідомлення оператору-донору / базовому оператору і заявка про перенесення номера відхиляється.

Процес повернення номера передбачає наступну послідовність:

1) абонент подає заявку оператору-отримувачу з проханням розірвати договір;

2) оператор-отримувач формує та передає до АІС ЦБД ПН повідомлення про відключення перенесеного номера;

3) АІС ЦБД ПН підтверджує повідомлення та надсилає його оператору-донору;

4) оператор-донор повинен підтвердити повернення номера і повідомити про це, надіславши до АІС ЦБД ПН підтверджуючий запит;

5) АІС ЦБД ПН пересилає повідомлення про підтвердження повернення номера оператору-отримувачу і повідомляє усіх операторів про повернення номера.

Деталізовані описи зазначених процесів наведені в ТЗ на проектування, розроблення та впровадження Автоматизованої інформаційної системи "Централізована база даних перенесених номерів".

3.6 Характеристики фізичного середовища

3.6.1 Фізичне розташування АІС ЦБД ПН

ОЦОД розміщується за адресою: м. Київ, вул. Смоленська, 31-33, технічний майданчик ПрАТ "ДАТАГРУП".

РЦОД розміщується за адресою: м. Київ, просп. Перемоги, 151, ДП "Український державний центр радіочастот".

РС Адміністратора АІС ЦБД ПН розміщуються в службових приміщеннях ДП "Український державний центр радіочастот".

Робоче місце віддаленого адміністрування розміщується в службовому приміщенні суб'єкта господарювання (резидента України), який забезпечує технічну підтримку (супроводження) прикладного програмного забезпечення АІС ЦБД ПН.

3.6.2 Контрольно-пропускний режим

Вхід в будівлі, де розміщені компоненти АІС ЦБД ПН, здійснюється через пропускні пункти, обладнані турнікетами, за персональними перепустками працівників або тимчасовими перепустками відвідувачів.

3.6.3 Режим доступу до приміщень

В приміщеннях, в яких розташовані компоненти АІС ЦБД ПН, діє пропускний та внутрішньооб'єктовий режими. Перелік осіб, що мають право доступу до апаратних та програмних засобів ОЦОД/РЦОД, визначається керівництвом ДП "Український державний центр радіочастот". Доступ інших осіб в такі приміщення можливий лише в супроводі осіб, яким надано право такого доступу.

3.7 Характеристики користувачів

3.7.1 Категорії користувачів

За рівнем повноважень щодо доступу до інформації та характером робіт, що виконуються у процесі забезпечення функціонування АІС ЦБД ПН, особи, які мають доступ до її ресурсів, поділяються на такі категорії:

1) *системний адміністратор* – користувач, який здійснює управління системними налаштуваннями апаратних та програмних засобів АІС ЦБД ПН;

2) *адміністратор безпеки* – користувач, який здійснює управління обліковими записами користувачів всіх категорій АІС ЦБД ПН (прикладному та системному програмному забезпеченні) та налаштуваннями обладнання мережевої безпеки АІС ЦБД ПН;

3) *віддалений адміністратор* – користувач, який здійснює віддалене управління налаштуваннями прикладного програмного забезпечення АІС ЦБД ПН на підставі відповідного договору з технічної підтримки (супроводження);

4) *користувач УДЦР* – співробітник ДП "Український державний центр радіочастот", який забезпечує підтримку інформаційного обміну між

операторами телекомунікацій при виконанні ППН, обробку інформації, яка зберігається в ЦБД ПН;

5) *користувач оператора телекомунікацій* – співробітник оператора телекомунікацій, який забезпечує виконання технологічних процедур, пов'язаних із реалізацією ППН;

6) *користувач інформаційних послуг АІС ЦБД ПН* – співробітник державного органу або суб'єкта господарювання, який використовує дані про перенесені абонентські номери у власних технологічних процесах;

7) *постачальники та розробники* апаратних засобів та прикладного програмного забезпечення АІС ЦБД ПН, що забезпечують їх технічну підтримку, а в разі необхідності їх модернізацію.

Усі користувачі АІС ЦБД ПН, в залежності від категорії, повинні мати відповідну підготовку щодо експлуатації апаратних та програмних засобів АІС ЦБД ПН для забезпечення виконання своїх службових та функціональних обов'язків.

Забороняється суміщення ролей адміністраторів АІС ЦБД ПН та користувачів АІС ЦБД ПН.

3.7.2 Розподіл обов'язків адміністраторів АІС ЦБД ПН

Розподіл обов'язків адміністраторів АІС ЦБД ПН повинен здійснюватися на основі функціональних задач, які виконують адміністратори. В АІС ЦБД ПН встановлено наступні ролі адміністраторів:

1) системний адміністратор, що здійснює адміністрування апаратних та програмних засобів АІС ЦБД ПН;

2) адміністратор безпеки, що здійснює управління обліковими записами користувачів та їх правами доступу до інформаційних об'єктів АІС ЦБД ПН, налаштування обладнання мережевої безпеки АІС ЦБД ПН;

3) віддалений адміністратор, що здійснює віддалене управління налаштуваннями прикладного програмного забезпечення АІС ЦБД ПН.

3.8 Особливості функціонування

Режим роботи АІС ЦБД ПН – цілодобовий. Виконання робіт, пов'язаних з регламентним технічним обслуговуванням компонентів АІС ЦБД ПН, здійснюється у порядку, визначеному відповідною експлуатаційною, технічною документацією та включається до Плану захисту інформації в АІС ЦБД ПН.

3.9 Клас АІС ЦБД ПН

АІС ЦБД ПН відноситься до інформаційно-телекомунікаційних систем класу "3" (згідно з НД ТЗІ 2.5-005-99).

3.10 Опис загроз інформації, що циркулює в АІС ЦБД ПН

При аналізі загроз, які існують для АІС ЦБД ПН, основне припущення повинно робитись з врахуванням того, що користувач, який має повний

адміністративний доступ до компонентів системи і фізичний доступ до комутаційного та серверного обладнання, не розглядається в якості потенційного порушника. Технічні заходи, описані в цьому ТЗ, що спрямовані на захист від зловмисних дій користувачів з адміністративними правами, розглядаються як додаткові. В якості основних заходів для захисту від загроз розглядаються організаційні заходи (кадрова політика, взаємний контроль адміністраторів при виконанні важливих технологічних операцій).

Неформалізований опис загроз, що вважаються найбільш актуальними для АІС ЦБД ПН, наведений в п.п. 3.10.1 – 3.10.3 ТЗ.

Якісна оцінка імовірності реалізації загроз та умовні втрати внаслідок їх реалізації зроблена за чотирирівневою шкалою (низький, середній, високий, дуже високий), визначений сукупний рівень загрози.

При цьому при розроблення КСЗІ повинні братись до уваги тільки загрози з середнім та високим ефективним рівнем.

Деталізовані відомості щодо моделі загроз інформації в АІС ЦБД ПН та моделі порушника повинні бути наведені в окремому документі "Модель загроз для інформації в АІС ЦБД ПН".

Оскільки неможливо одержати достатньо об'єктивні дані про імовірність реалізації більшості з загроз, перелічених в п.п. 3.10.1 – 3.10.3 ТЗ, імовірність реалізації загроз визначено експертним методом та, для окремих загроз, що є типовими для ІТС класу "3", емпіричним шляхом з врахуванням досвіду експлуатації подібних систем.

3.10.1 Загрози конфіденційності інформації

3.10.1.1 Порушення конфіденційності інформації, що обробляється та зберігається в АІС ЦБД ПН

Розглядаються наступні шляхи порушення конфіденційності інформації, що обробляється та зберігається в АІС ЦБД ПН (відкрита та конфіденційна інформація, перелічена в таблиці 3.1).

К.1.1 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок несанкціонованого фізичного доступу до обладнання.

Імовірність реалізації: середня
Втрати внаслідок реалізації: високі
Ефективний рівень: високий

К.1.2 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, під час її обробки внаслідок навмисного підключення до обладнання, помилок при налаштуванні технічних засобів телекомунікацій або апаратних збоїв.

Імовірність реалізації: низька
Втрати внаслідок реалізації: високі
Ефективний рівень: середній

К.1.3 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок

навмисного підключення до каналів зв'язку чи обладнання з наступним використанням для несанкціонованого доступу відомих вразливостей програмно-технічних засобів АІС ЦБД ПН.

Імовірність реалізації: низька
Втрати внаслідок реалізації: високі
Ефективний рівень: середній

К.1.4 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок навмисного підключення до каналів зв'язку чи обладнання з наступним використанням для несанкціонованого доступу перехоплених атрибутів доступу авторизованих користувачів.

Імовірність реалізації: низька
Втрати внаслідок реалізації: високі
Ефективний рівень: середній

К.1.5 Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня
Втрати внаслідок реалізації: високі
Ефективний рівень: високий

3.10.1.2 Порушення конфіденційності технологічної інформації

К.2.1 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) сторонніми особами внаслідок необережного поводження авторизованих користувачів з атрибутами доступу (розглядається в якості частини реалізації атак **К.1.1**, **К.1.4**, спрямованих на порушення конфіденційності інформації).

Імовірність реалізації: середня
Втрати внаслідок реалізації: середні
Ефективний рівень: середній

К.2.2 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) зі сторони авторизованих користувачів системи внаслідок необережного поводження з ними (як мета такого порушення розглядається ескалація прав доступу до ресурсів АІС ЦБД ПН та виконання несанкціонованих дій від імені іншого користувача, розглядається в якості частини атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока
Втрати внаслідок реалізації: середні
Ефективний рівень: високий

К.2.3 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів системи) зі сторони авторизованих користувачів системи з застосуванням відомих вразливостей програмно-технічних засобів АІС ЦБД

ПН (розглядається в якості частини атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока
Втрати внаслідок реалізації: середні
Ефективний рівень: високий

К.2.4 Отримання несанкціонованого доступу сторонніх осіб до технологічної інформації (атрибути доступу, конфігураційні налаштування), що зберігається та обробляється в АІС ЦБД ПН, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня
Втрати внаслідок реалізації: низькі
Ефективний рівень: середній

3.10.2 Загрози цілісності інформації

3.10.2.1 Загрози цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН

Ц.1.1 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок апаратного або програмного збою.

Імовірність реалізації: середня
Втрати внаслідок реалізації: дуже високі
Ефективний рівень: високий

Ц.1.2 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, сторонніми особами внаслідок отримання фізичного доступу до обладнання (навмисне чи внаслідок необережного поводження з обладнанням, що забезпечують його функціонування).

Імовірність реалізації: низька
Втрати внаслідок реалізації: високі
Ефективний рівень: середній

Ц.1.3 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок навмисних дій авторизованого користувача будь-якого рівня в межах його повноважень.

Імовірність реалізації: середня
Втрати внаслідок реалізації: дуже високий
Ефективний рівень: високий

Ц.1.4 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок ненавмисних (помилкових) дій авторизованого користувача будь-якого рівня.

Імовірність реалізації: середня
Втрати внаслідок реалізації: середні
Ефективний рівень: середній

Ц.1.5 Порушення цілісності інформації, що обробляється та зберігається в АІС ЦБД ПН, внаслідок ураження шкідливим ПЗ.

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні
Ефективний рівень: середній

3.10.2.2 Загрози цілісності технологічної інформації

Ц.2.1 Порушення цілісності технологічної інформації (журнали реєстрації подій) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів АІС ЦБД ПН або перехоплених атрибутів доступу користувачів АІС ЦБД ПН з адміністративними правами (як мета реалізації даної загрози розглядається приховування несанкціонованих дій в системі в рамках реалізації інших загроз, спрямованих на порушення цілісності або конфіденційності інформації).

Імовірність реалізації: низька
Втрати внаслідок реалізації: високі
Ефективний рівень: середній

Ц.2.2 Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів АІС ЦБД ПН або перехоплених атрибутів доступу користувачів АІС ЦБД ПН з адміністративними правами (як мета реалізації даної загрози розглядається створення умов для подальшого несанкціонованого доступу до інших компонент системи в рамках реалізації загроз **К.1.1** – **К.1.4**, **Ц.2.1** (для сторонніх осіб), **Ц.1.3** (для авторизованих користувачів)).

Імовірність реалізації: низька
Втрати внаслідок реалізації: середні
Ефективний рівень: середній

Ц.2.3 Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) внаслідок ураження системи шкідливим ПЗ.

Імовірність реалізації: низька
Втрати внаслідок реалізації: середні
Ефективний рівень: середній

3.10.3 Загрози доступності інформації

3.10.3.1 Загрози доступності інформації, що зберігається в АІС ЦБД ПН

Д.1.1 Втрата доступності інформації, що зберігається в АІС ЦБД ПН, внаслідок виходу з ладу комутаційного або серверного обладнання, або елементів, що їх забезпечують (найбільш імовірним вважається вихід з ладу системи електроживлення).

Імовірність реалізації: висока
Втрати внаслідок реалізації: низькі
Ефективний рівень: середній

Д.1.2 Втрата доступності інформації, що зберігається в АІС ЦБД ПН, внаслідок ураження системи шкідливим ПЗ (перевантаження каналів зв'язку віддалених користувачів інтенсивним трафіком, що генерується вірусами типа "хробак", при розповсюдженні, вичерпання дискового простору або

процесорного часу на уражених деякими типами шкідливого програмного забезпечення серверах, що призводить до неможливості обробки запитів та виникненні відмов в обслуговуванні).

Імовірність реалізації: середня
Втрати внаслідок реалізації: низькі
Ефективний рівень: середній

4 ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Загальні вимоги до реалізації політики безпеки

4.1.1 Принцип створення КСЗІ

Згідно з положеннями ДСТУ 3396.1-96, КСЗІ в АІС ЦБД ПН створюється за принципом досягнення необхідного рівня захисту інформації за допустимих затрат і заданого рівня обмежень видів інформаційної діяльності.

4.1.2 Організаційна структура управління КСЗІ

З метою організаційного забезпечення завдань керування КСЗІ в АІС ЦБД ПН та здійснення контролю за її функціонуванням, виконання робіт з визначення вимог із захисту інформації в АІС ЦБД ПН, проектування, розроблення і модернізації КСЗІ, а також для експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації створюється служба захисту інформації (СЗІ) щонайменше у такому складі:

- керівник СЗІ;
- системний адміністратор;
- адміністратор безпеки.

Дозволяється за необхідності здійснювати суміщення зазначених посад із іншими штатними посадами ДП "Український державний центр радіочастот" за умови якісного та вчасного виконання посадовими особами своїх функціональних обов'язків. Забороняється суміщення ролей адміністраторів АІС ЦБД ПН та користувачів АІС ЦБД ПН.

Віддалений адміністратор призначається зі складу персоналу організації, яка здійснює технічну підтримку (супроводження) прикладного програмного забезпечення АІС ЦБД ПН.

4.1.3 Керування доступом користувачів до інформації

В АІС ЦБД ПН реалізується адміністративний принцип керування доступом. Потоки інформації всередині АІС ЦБД ПН встановлюються адміністратором безпеки і не можуть бути змінені іншими користувачами. В АІС ЦБД ПН виділена посада системного адміністратора, повноваження та обов'язки якого зафіксовані в посадовій інструкції.

Системний адміністратор відповідає за управління системними налаштуваннями апаратних та програмних засобів, платформи віртуалізації, технічних засобів телекомунікацій ОЦОД та РЦОД АІС ЦБД ПН.

Адміністратор безпеки відповідає за управління обліковими записами користувачів всіх категорій АІС ЦБД ПН (прикладного та системного програмного забезпечення) та налаштування обладнання мережевої безпеки ОЦОД та РЦОД АІС ЦБД ПН.

Розмежування доступу до об'єктів захисту адміністраторів та користувачів АІС ЦБД ПН здійснюється штатними засобами системного та

прикладного програмного забезпечення, а також технічними засобами телекомунікацій відповідно до налаштувань, визначених адміністратором безпеки.

4.1.4 Підходи щодо адміністрування КЗЗ

Управління комплексом засобів захисту (КЗЗ) та технічними засобами телекомунікацій, що входять до складу АІС ЦБД ПН, а також моніторинг їх стану здійснюється з використанням локального або віддаленого доступу до відповідного обладнання.

4.1.5 Правила розмежування інформаційних потоків

Категорії користувачів, що повинні бути визначені в АІС ЦБД ПН, та правила розмежування доступу визначених категорій користувачів до інформації, що підлягає захисту, викладені в п. 3.7.1 ТЗ.

4.1.6 Вимоги до взаємодії

Взаємодія ОЦОД та РЦОД АІС ЦБД ПН забезпечується з використанням мережі Інтернет шляхом фізичного підключення до неї технічних засобів телекомунікацій виключно через засоби криптографічного захисту інформації. Додатково з метою захисту від мережевих атак в складі ОЦОД та РЦОД використовуються міжмережеві екрани (п.п. 3.2.1, 3.2.2 ТЗ).

Підключення ІТС операторів телекомунікацій, державних органів, суб'єктів господарювання, а також робочого місця віддаленого адміністрування повинно здійснюватись в порядку, визначеному в Типовому організаційно-технічному рішенні з підключення ІТС та РС операторів телекомунікацій, державних органів та інших суб'єктів господарювання до АІС ЦБД ПН ІТС, затвердженому наказом ДП "Український державний центр радіочастот" № 325 від 26.05.2017.

Забезпечення захисту інформації в процесі взаємодії АІС ЦБД ПН з ІТС операторів телекомунікацій, державних органів, суб'єктів господарювання повинно здійснюватися виключно відповідно до типових організаційно-технічних рішень з підключення до АІС ЦБД ПН з використанням засобів криптографічного захисту інформації.

4.1.7 Основні атрибути доступу користувачів, процесів і об'єктів

Основними атрибутами доступу користувачів, що використовуються для проведення ідентифікації, автентифікації та авторизації КЗЗ, є:

– умовний ідентифікатор в АІС ЦБД ПН (логін);
– пароль.

Атрибутами інформаційних об'єктів, що використовуються для розмежування доступу, є:

– в файлових системах: ім'я, розширення, атрибути доступу (читання, модифікація, знищення);

– для об'єктів баз даних: ім'я об'єкта, атрибути доступу (читання, вставка, модифікація, знищення);

– при передачі інформаційних об'єктів засобами обчислювальної мережі додатковими атрибутами, за якими виконують розмежування доступу мережеві засоби захисту, є: IP-адреса відправника IP-пакету, IP-адреса отримувача IP-пакету, TCP/UDP-порт прикладного процесу-відправника, TCP/UDP-порт прикладного процесу-отримувача, номер пакету у послідовності (тільки для TCP), значення, визначені в службових полях заголовків різних рівнів (TTL, прапори та ін.), команда протоколу прикладного рівня.

Атрибутами локальних процесів є:

– назва виконуваного програмного модуля;

– ідентифікатор процесу в операційній системі.

Для процесів, що призначені для мережевої взаємодії, додатковими атрибутами, за якими виконують розмежування доступу мережеві засоби захисту, є:

– тип протоколу транспортного рівня, що використовується процесом;

– TCP/UDP–порт (діапазон портів) призначення;

– TCP/UDP–порт (діапазон портів) відправника;

– тип протоколу прикладного рівня, що використовується процесом.

4.1.8 Вимоги до реєстрації подій в АІС ЦБД ПН

КЗЗ АІС ЦБД ПН повинен забезпечити виконання вимог із забезпечення спостережності та контрольованості технологічних процесів в АІС ЦБД ПН.

4.1.8.1 Вимоги до реєстрації дій користувачів по відношенню до інформації, яка обробляється та зберігається в АІС ЦБД ПН

Н.1.1 КЗЗ повинен дозволяти однозначно ідентифікувати користувача, що сформував запит на будь-яку дію, пов'язану зі зміною інформації, яка зберігається в базі даних (створення, модифікація, знищення), та відстежити історію таких транзакцій.

4.1.8.2 Вимоги до реєстрації дій користувачів по відношенню до технологічної інформації.

Н.2.1 Отримання авторизованими користувачами доступу до АІС ЦБД ПН (вхід/вихід).

Н.2.2 Невдалі спроби отримання доступу до будь-якого компоненту АІС ЦБД ПН внаслідок непроходження користувачем автентифікації.

Н.2.3 Зміни конфігураційних налаштувань компонент АІС ЦБД ПН (серверів та мереженого обладнання).

Н.2.4 Отримання авторизованими користувачами доступу до об'єктів захисту АІС ЦБД ПН.

4.2 Загальні вимоги до КСЗІ

Для забезпечення захисту від загроз, визначених в п. 3.10 ТЗ, компоненти КСЗІ повинні реалізовувати наступні основні функції захисту:

1) забезпечення стійкості АІС ЦБД ПН в цілому до відмов та унеможливлення втрати інформації, що повинно забезпечуватися шляхом резервування елементів системи збереження даних, засобів комутації та електроживлення. Також повинно забезпечуватися резервне копіювання ЦБД ПН, програмного забезпечення АІС ЦБД ПН. Необхідна періодичність резервного копіювання, порядок відновлення з резервних копій та відповідальність за збереження носіїв резервних копій визначається на етапі проектування та відображається у відповідних інструкціях системного адміністратора (захист від загроз Ц.1.1, Ц.1.2, Ц.1.3, Ц.1.5, Д.1.1, Д.1.2);

2) розмежування доступу користувачів АІС ЦБД ПН до інформації, що зберігається в базі даних, відповідно до їх повноважень згідно з технологічним процесом обробки інформації (захист від загроз К.2.1, К.2.2, К.2.3, Ц.1.3, Ц.2.2);

3) забезпечення однозначної ідентифікації користувачів АІС ЦБД ПН (забезпечення Н.1.1);

4) забезпечення можливості відстеження історії запитів, спрямованих на внесення змін до інформації, що зберігаються в базі даних АІС ЦБД ПН, та однозначної ідентифікації користувачів АІС ЦБД ПН, що виконували такі зміни, а саме: внесення, модифікація, видалення (забезпечення Н.1.1, Н.2.1);

5) забезпечення скасування (відкату) обмеженої кількості останніх транзакцій, що виконані користувачем. Кількість транзакцій, що можуть бути відмінені визначається на етапі проектування (захист від загроз Ц.1.4);

6) забезпечення захисту від несанкціонованого доступу до інформації при її обробці засобами АІС ЦБД ПН організаційними заходами (захист від загроз К.1.1, К.1.2, К.1.3, К.1.4, К.1.5, К.2.4);

7) забезпечення реєстрації подій, пов'язаних з отриманням користувачами доступу до ресурсів АІС ЦБД ПН (проходження/непроходження автентифікації), дій системного адміністратора та адміністратора безпеки щодо зміни налаштувань серверів та мережевого обладнання (забезпечення Н.2.3, Ц.2.1);

8) наявність засобів перегляду та аналізу подій (забезпечення Н.1.1, Н.2.1 – Н.2.4);

9) наявність засобів для резервування конфігураційних файлів та критично важливих для функціонування обладнання АІС ЦБД ПН системних файлів (створення образів дисків, резервування операційних систем та програмного забезпеченння серверів, об'єктів системи віртуалізації та активного мережевого обладнання) з метою їх наступного швидкого відновлення в разі збоїв (захист від загроз Ц.2.3);

10) забезпечення антивірусного захисту (захист від загроз Ц.1.5, Ц.2.3, Д.1.2) в обсязі: в АІС ЦБД ПН повинні використовуватись засоби антивірусного захисту; повинні передбачатись процедури оновлення антивірусних баз; оновлення повинне здійснюватися в автоматичному або

ручному режимі; порядок оновлення антивірусних баз повинен бути визначений на етапі проектування та наведений в нормативно-розпорядчій документації на КСЗІ;

11) інсталяція програмного забезпечення на ЕОМ із складу АІС ЦБД ПН або відновлення (відкат) системних та конфігураційних файлів з резервних копій повинно здійснюватись тільки з контрольних дистрибутивних пакетів, що зберігаються системним адміністратором;

12) визначення порядку дій користувачів у випадку відмови КСЗІ (окремого її модуля, компонента) в Плані захисту інформації в АІС ЦБД ПН;

13) визначення організації захисту інформації в АІС ЦБД ПН в Плані захисту інформації в АІС ЦБД ПН.

4.3 Вимоги до фізичного середовища

Вхід до приміщень, в яких розміщуються компоненти АІС ЦБД ПН, повинен бути обмежений, доступ працівників повинен контролюватись охороною.

Серверне обладнання ЦОД АІС ЦБД ПН повинно розташовуватись в окремому виділеному приміщенні з метою мінімізації доступу до приміщення осіб, що не мають відношення до обслуговування та експлуатації такого обладнання.

Доступ до виділеного приміщення повинен бути обмежений. Перелік осіб, які мають доступ до цього приміщення, визначається керівництвом ДП "Український державний центр радіочастот". За необхідності доступу до серверного приміщення відвідувачів, останні повинні знаходитися в приміщеннях тільки у супроводженні працівника, який визначений наведеним вище чином.

Приміщення, в яких розташовані компоненти АІС ЦБД ПН, повинні бути обладнані системами вентиляції. Повинно здійснюватись постійне зовнішнє спостереження за приміщеннями з метою раннього виявлення ознак, що можуть призвести до несанкціонованого доступу.

Розміщення компонентів АІС ЦБД ПН має виконуватися, виходячи з:

– блокування можливості витоку інформації, що циркулює в АІС ЦБД ПН, мережевими каналами зв'язку з використанням обладнання мережевого захисту;

– технічних характеристик обладнання і вимог щодо його встановлення та умов експлуатації, визначених їх виробником.

4.4 Вимоги до користувачів

Користувачі категорій 1 – 6 (п. 3.7.1 ТЗ) повинні мати належний рівень кваліфікації і володіти навичками для виконання робіт відповідно до покладених на них завдань.

Користувачі категорій 1 – 6 повинні пройти процедуру реєстрації в АІС ЦБД ПН і мати особисті облікові записи та атрибути доступу.

Користувачі категорії 7 повинні мати дозвіл на доступ до відомостей, які містяться в технічній документації на КСЗІ або окремих її компонентах, необхідних для виконання функціональних обов'язків, виконання робіт із тестування та інсталяції програмного забезпечення АІС ЦБД ПН, встановлення і регламентного обслуговування обладнання тощо.

4.5 Вимоги до організаційного забезпечення

Експлуатація АІС ЦБД ПН повинна здійснюватись лише за умови наявності затвердженого у встановленому порядку Плану захисту інформації в АІС ЦБД ПН.

Дії користувачів категорій 1 – 6 (п. 3.7.1 ТЗ) повинні визначатися відповідними настановами (інструкціями).

Повинні бути розроблені порядок дій користувачів категорії 1 – 3 у разі відмови КСЗІ (окремого її компоненту) та затверджені відповідні настанови кожного користувача. Ці документи повинні бути складовими Плану захисту інформації в АІС ЦБД ПН.

Повинні бути розроблені нормативні та розпорядчі документи, що визначають правила режиму доступу у приміщення, в яких розміщені компоненти АІС ЦБД ПН, та порядок доступу відвідувачів до цих компонентів.

4.6 Вимоги до КСЗІ в частині захисту від несанкціонованого доступу

КЗЗ АІС ЦБД ПН повинен забезпечити реалізацію профілю захищеності інформації: {КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-3, НЦ-1, НВ-1}.

КЗЗ АІС ЦБД ПН повинен забезпечити виконання наступних функцій із захисту інформації, що циркулює в АІС ЦБД ПН:

– захист конфіденційності та цілісності інформації, яка циркулює в АІС ЦБД ПН, від несанкціонованого доступу та модифікації;

– забезпечення доступності інформації, яка циркулює в АІС ЦБД ПН, для авторизованих користувачів;

– захист конфіденційності, цілісності та доступності технологічної інформації АІС ЦБД ПН, яка повинна бути доступна тільки уповноваженому персоналу, що забезпечує встановлення, налаштування та управління програмними та технічними засобами АІС ЦБД ПН;

– ідентифікацію, автентифікацію та авторизацію користувачів АІС ЦБД ПН;

– розмежування та контроль доступу користувачів до інформаційних ресурсів та сервісів АІС ЦБД ПН;

– забезпечення спостережності за діями користувачів в АІС ЦБД ПН;

– реєстрацію всіх подій в АІС ЦБД ПН, які мають відношення до безпеки інформації, та їх аудит;

– захист конфіденційності та цілісності інформації, яка передається незахищеними каналами зв'язку.

4.6.1 Об'єкти захисту

Об'єктами захисту є дані, сукупність даних певної логічної структури (файл, база даних) АІС ЦБД ПН, в яких знаходиться інформація, що підлягає захисту, а також програмне забезпечення, що реалізує технології оброблення такої інформації, для виконання АІС ЦБД ПН своїх функцій.

Об'єкти захисту поділені відповідно до функціонального призначення, місця розміщення та виду представлення в АІС ЦБД ПН наведені в таблиці 4.1.

Таблиця 4.1 – Поділ об'єктів захисту

Об'єкт захисту	Умовне позначення	Вигляд представлення
Операційні системи, прикладне та спеціалізоване програмне забезпечення АРМ та серверів АІС ЦБД ПН	{SOFT}	У вигляді файлів
Журнали реєстрації подій системного програмного забезпечення АІС ЦБД ПН в електронній формі	{SOFT-LOG}	У вигляді файлів
Журнали реєстрації подій прикладного програмного забезпечення АІС ЦБД ПН в електронній формі	{DB-LOG}	У вигляді об'єктів бази даних
Дані про план нумерації	{PLAN}	У вигляді файлів та об'єктів бази даних
Дані про перенесені номери (повний список перенесених номерів, інкрементальний список перенесених номерів, список повернених номерів)	{NUM}	
Блок зашифрованих даних в заявці на перенесення номеру	{REQ-PERS}	У складі xml-файлів спеціалізованого формату
Відкриті технологічні дані, що містяться в заявках на перенесення номера	{REQ-DATA}	
Статистична інформація про виконання ППН	{STAT}	
Резервні копії інформації, що зберігається в базах даних; резервні копії програмного забезпечення	{DB-BACKUP}	У вигляді файлів
Конфігураційні та системні об'єкти складових елементів АІС ЦБД ПН, що визначають параметри конфігурації, функціонування та правила розмежування доступу	{SOFT-CFG}	У вигляді файлів
Конфігураційні та системні об'єкти прикладного програмного забезпечення АІС ЦБД ПН	{DB-CFG}	У вигляді файлів та об'єктів баз даних
Конфігураційні та системні об'єкти складових елементів АІС ЦБД ПН, що визначають правила розмежування доступу	{SEC-CFG}	У вигляді файлів

В таблиці 4.2 наведені властивості із захисту інформації, які повинні забезпечуватись для відповідних об'єктів захисту, зазначених в таблиці 4.1, зі сторони КЗЗ АІС ЦБД ПН.

Таблиця 4.2 – Вимоги щодо забезпечення властивостей інформації

Вид інформації (згідно з таблицею 4.1)	**Вимоги щодо забезпечення властивостей інформації**			
	конфіденційність	**цілісність**	**доступність**	**спостережність**
{SOFT}	-	+	+	+
{SOFT-LOG}	+	+	+	+
{DB-LOG}	+	+	+	+
{PLAN}	+	+	+	+
{NUM}	+	+	+	+
{REQ-PERS}	+	+	+	+
{REQ-DATA}	-	+	+	+
{STAT}	+	+	+	+
{DB-BACKUP}	+	+	+	+
{SOFT-CFG}	+	+	+	+
{DB-CFG}	+	+	+	+
{SEC-CFG}	+	+	+	+

4.6.2 Суб'єкти доступу

Суб'єктами доступу до ресурсів АІС ЦБД ПН є її користувачі відповідно до п. 3.7.1 ТЗ.

За рівнем повноважень щодо доступу до технічних та програмних засобів, інформації, що циркулює та накопичується в АІС ЦБД ПН, характером та змістом робіт, які виконуються в процесі функціонування, суб'єкти доступу поділяються на групи, наведені в таблиці 4.3.

Таблиця 4.3 – Суб'єкти доступу до ресурсів АІС ЦБД ПН

Суб'єкт доступу	**Умовне позначення**
Системний адміністратор	[А_СА]
Адміністратор безпеки	[А_АБ]
Віддалений адміністратор	[А_АВ]
Користувач УДІЦР	[О_У]
Користувач оператора телекомунікацій	[О_Т]
Користувачів інформаційних послуг АІС ЦБД ПН	[О_К]
Розробники програмного забезпечення та постачальники апаратного забезпечення АІС ЦБД ПН	[К_РП]

4.6.3 Взаємодія суб'єктів і об'єктів

Взаємодія суб'єктів доступу і об'єктів захисту АІС ЦБД ПН здійснюється згідно з атрибутами доступу, що їм належать. Атрибути доступу повинні визначатись згідно з п. 4.1.7 ТЗ.

Взаємодія суб'єктів доступу і об'єктів захисту в АІС ЦБД ПН здійснюється згідно з адміністративним принципом керування доступом.

Загальні правила розмежування доступу користувачів до ресурсів АІС ЦБД ПН визначаються згідно з таблицею 4.4.

Таблиця 4.4 – Розмежування доступу користувачів до ресурсів АІС ЦБД ПН

Об'єкт доступу	**Суб'єкт доступу**						
	[А_СА]	**[А_АБ]**	**[А_АВ]**	**[О_У]**	**[О_Т]**	**[О_К]**	**[К_РП]**
{SOFT}	+	+	+	+			+
{SOFT-LOG}	+	+	+				+
{DB-LOG}	+	+	+				+
{PLAN}	+	+	+	+	+		
{NUM}	+	+	+	+	+	+	
{REQ-PERS}					+		
{REQ-DATA}	+	+	+	+	+		
{STAT}	+	+	+	+		+	
{DB-BACKUP}	+		+				
{SOFT-CFG}	+		+				
{DB-CFG}	+	+	+				
{SEC-CFG}		+					

Примітка. В таблиці 4.4 знаком "+" визначено наявність права доступу певної категорії користувачів до інформаційних, програмних та апаратних ресурсів АІС ЦБД ПН. У першій графі таблиці зазначені інформаційні та технічні ресурси, доступ до яких контролюється. В таблиці 4.4 використовуються коди інформаційних ресурсів та суб'єктів доступу до них, що приведені в п.п. 4.6.1 та 4.6.2 ТЗ.

Суб'єкти повинні одержувати права щодо типу доступу до об'єктів згідно з правилами, визначеними у таблиці 4.5.

Таблиця 4.5 – Типи доступу суб'єктів доступу до об'єктів доступу

Суб'єкт	**Тип доступу**			
	читання	**модифікація**	**створення**	**видалення**
[А_СА]	{SOFT} {SOFT-LOG} {DB-LOG} {PLAN} {NUM} {REQ-DATA} {STAT} {DB-BACKUP} {SOFT-CFG} {DB-CFG}	{NUM} {REQ-DATA} {SOFT-CFG}	{SOFT} {SOFT-LOG} {REQ-DATA} {DB-BACKUP} {SOFT-CFG}	{SOFT} {SOFT-LOG} {REQ-DATA} {NUM} {DB-BACKUP} {SOFT-CFG}
[А_АБ]	{SOFT} {SOFT-LOG} {DB-LOG} {PLAN} {NUM} {REQ-DATA} {CERT} {SEC-CFG} {DB-CFG}	{SEC-CFG}		
[А_АВ]	{SOFT}	{DB-CFG}		

Суб'єкт	Тип доступу			
	читання	**модифікація**	**створення**	**видалення**
	{SOFT-LOG} {DB-LOG} {PLAN} {NUM} {REQ-DATA} {STAT} {DB-BACKUP} {SOFT-CFG} {DB-CFG}			
[О_У]	{SOFT} {PLAN} {NUM} {REQ-DATA} {STAT}	{PLAN}	{PLAN}	{PLAN}
[О_Т]	{PLAN} {NUM} {REQ-PERS} {REQ-DATA}	{REQ-PERS} {REQ-DATA}	{REQ-PERS} {REQ-DATA}	{REQ-PERS} {REQ-DATA}
[О_К]	{NUM} {STAT}			
[К_РП]	{SOFT} {SOFT-LOG} {DB-LOG}	{SOFT}		

Примітки:

1) Під видом доступу "читання" для об'єкту {SOFT} розуміється доступ на запуск відповідного процесу.

2) Окремі правила розмежування доступу можуть уточнюватись при виконанні робіт зі створення КСЗІ.

Спеціалісти, які здійснюють розробку та супроводження програмного забезпечення, заміну або модернізацію апаратних засобів АІС ЦБД ПН [К_РП], можуть отримати права доступу, визначені в таблиці 4.5, лише на момент проведення необхідних робіт. Виконання цих робіт здійснюється під контролем системного адміністратора або адміністратора безпеки.

Надання користувачу певної ролі, атрибутів доступу до певного ресурсу та його прав по доступу повинно здійснюватися тільки при виконанні таких умов:

– категорія користувача відповідає типу об'єкта захисту згідно з загальними правилами розмежування доступу (таблиця 4.5);

– доступ до даного об'єкта захисту визначено службовими обов'язками користувача;

– вид взаємодії користувача з об'єктом захисту (перелік дій над об'єктом) дозволено специфікаціями послуг безпеки (таблиця 4.5);

– вид взаємодії користувача з об’єктом захисту (тип доступу) визначено службовими обов’язками користувача.

4.6.4 Вимоги до послуг безпеки

Нижче наведений формалізований опис послуг безпеки, які повинен реалізувати КЗЗ АІС ЦБД ПН для забезпечення захисту від визначених в п. 3.8 ТЗ загроз в термінах НД ТЗІ 2.5-004-99. Взаємодія суб’єктів доступу і об’єктів захисту АІС ЦБД ПН здійснюється згідно з загальними правилами розмежування доступу (п. 4.6.3 ТЗ) на підставі відповідних атрибутів доступу (п. 4.1.7 ТЗ) та вимогами до основних функцій захисту (п. 4.2 ТЗ).

КЗЗ АІС ЦБД ПН повинен забезпечувати наступний функціональний профіль захисту: {КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-3, НЦ-1, НВ-1}.

4.6.4.1 Специфікації послуги "Базова адміністративна конфіденційність (КА-2)"

КЗЗ в рамках реалізації послуги "КА-2" повинен реалізувати політику базової адміністративної конфіденційності по відношенню до інформаційних об’єктів, наведених в таблиці 4.2 (для яких визначаються вимоги до забезпечення конфіденційності).

КЗЗ повинен забезпечити розмежування доступу суб’єктів доступу, вказаних в таблиці 4.3, до об’єктів захисту, вказаних в таблиці 4.1, у відповідності до правил, наведених в таблицях 4.4, 4.5.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного інформаційного об’єкта, визначених в п. 4.1.7 ТЗ.

Запити на зміну прав доступу користувачів до об’єктів повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного захищеного об’єкта шляхом керування належністю користувачів і об’єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об’єкта.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного процесу, що належить системному або прикладному програмному забезпеченню, визначати конкретних користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

4.6.4.2 Специфікації послуги "Повна конфіденційність при обміні (КВ-1)"

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів при обміні

даними між складовими елементами АІС ЦБД ПН через незахищене середовище.

Всі інформаційні об’єкти, що передаються між складовими елементами АІС ЦБД ПН, повинні передаватись в захищеному (зашифрованому) вигляді. Користувачі не повинні мати можливість впливати на рівень захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і приймальника об'єкта, визначених в п. 4.1.7 ТЗ.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і джерела об'єкта, визначених в п. 4.1.7 ТЗ.

Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника, визначених в п. 4.1.7 ТЗ.

Для реалізації послуги повинен використовуватись програмний засіб криптографічного захисту інформації, який має експертний висновок в сфері криптографічного захисту інформації.

4.6.4.3 Специфікації послуги "Мінімальна адміністративна цілісність (ЦА-1)"

КЗЗ в рамках реалізації послуги "ЦА-1" повинен реалізувати наступну політику мінімальної адміністративної цілісності по відношенню до всіх інформаційних об’єктів, наведених в таблиці 4.2.

КЗЗ повинен забезпечити розмежування доступу суб’єктів доступу, вказаних в таблиці 4.3, до об’єктів захисту, вказаних в таблиці 4.1, у відповідності до правил, наведених в таблицях 4.4, 4.5.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного інформаційного об’єкта, визначених в п. 4.1.7 ТЗ.

Запити на зміну прав доступу користувачів до об’єктів повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного захищеного об’єкта шляхом керування належністю користувачів і об’єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об’єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

4.6.4.4 Специфікації послуги "Обмежений відкат (ЦО-1)"

Політика відкату, що реалізується КЗЗ, повинна відноситися до програмного забезпечення та об’єктів баз даних.

Відкат операцій над програмним забезпеченням АІС ЦБД ПН повинен здійснюватись шляхом використання штатних засобів відповідних операційних систем АІС ЦБД ПН. Відкат операцій над програмним забезпеченням АІС ЦБД ПН повинен здійснюватись системним адміністратором.

Відкат операцій над інформаційними об’єктами баз даних повинен здійснюватись шляхом використання штатних засобів систем управління базами даних АІС ЦБД ПН (механізм транзакцій). Відкат цих об’єктів повинен здійснюватись адміністратором безпеки.

Необхідний проміжок часу, протягом якого можливий відкат, та обсяг операцій, які можуть бути відмінені, визначаються на етапі технічного проекту.

4.6.4.5 Специфікації послуги "Базова цілісність при обміні (ЦВ-2)"

Політика цілісності при обміні, що реалізується КЗЗ, повинна відноситись до інформаційних об'єктів і існуючих інтерфейсних процесів при обміні даними між складовими елементами АІС ЦБД ПН через незахищене середовище.

Всі інформаційні об’єкти, що передаються між складовими елементами АІС ЦБД ПН, повинні передаватись в захищеному (зашифрованому з використанням імітовставки) вигляді. Користувачі не повинні мати можливість впливати на рівень захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання.

Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу, визначених в п. 4.1.7 ТЗ.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу, визначених в п. 4.1.7 ТЗ.

Для реалізації послуги повинен використовуватись програмний засіб криптографічного захисту інформації, який має експертний висновок в сфері криптографічного захисту інформації.

4.6.4.6 Специфікації послуги "Стійкість при обмежених відмовах (ДС-1)"

Політика стійкості до відмов, що реалізується КЗЗ, повинна полягати в наступному.

Не повинно призводити до погіршення якості обслуговування відмова апаратних засобів ОЦОД. При цьому АІС ЦБД ПН продовжує функціонування за рахунок використання РЦОД.

При настанні інших відмов допускається зниження якості обслуговування або припинення функціонування АІС ЦБД ПН взагалі.

Для реалізації послуги повинні використовуватись відповідні джерела безперебійного живлення.

Технічні засоби КЗЗ повинні мати засоби індикації та/або оповіщення системного адміністратора та адміністратора безпеки про відмову будь-якого захищеного компонента.

4.6.4.7 Специфікації послуги "Модернізація (ДЗ-1)"

Повинен бути розроблений порядок модернізації та оновлення апаратних та програмних компонентів АІС ЦБД ПН, який не призводить до зміни політики безпеки та необхідності повторної експертизи КСЗІ в сфері технічного захисту інформації. Повинні бути визначені повноваження системного адміністратора щодо модернізації та оновлення програмних та апаратних компонентів АІС ЦБД ПН.

Під час оновлення програмного забезпечення має бути автентифіковано джерело оновлення та перевірено цілісність оновлення.

4.6.4.8 Специфікації послуги "Ручне відновлення (ДВ-1)"

Політика відновлення, що реалізується КЗЗ, повинна описувати мінімальну множину типів відмов технічних засобів та програмного забезпечення АІС ЦБД ПН і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки.

Ручне відновлення повинно проводитись в наступних випадках:

– вихід з ладу запам'ятовуючих пристроїв або пошкодження внаслідок апаратного збою областей пам'яті, де зберігаються інформаційні об'єкти, що містять технологічну інформацію, необхідну для функціонування операційних систем компонентів АІС ЦБД ПН: системні та конфігураційні файли (відновлення працездатності здійснюється системним адміністратором та адміністратором безпеки шляхом заміни несправного обладнання та повторної інсталяції та налаштування програмного забезпечення);

– вихід з ладу запам'ятовуючих пристроїв, де зберігається база даних АІС ЦБД ПН (відновлення працездатності здійснюється шляхом заміни системним адміністратором несправного обладнання та відновлення бази даних з резервних копій);

– вихід з ладу іншого апаратного забезпечення АІС ЦБД ПН (відновлення працездатності здійснюється системним адміністратором та адміністратором безпеки шляхом заміни несправного обладнання та повторного його налаштування).

Рівні відмов, у разі перевищення яких необхідна повторна інсталяція програмного забезпечення, визначаються на етапі проектування АІС ЦБД ПН.

Після відмови АІС ЦБД ПН або переривання обслуговування, КЗЗ повинен перевести АІС ЦБД ПН до стану, з якого повернути її в режим нормального функціонування може тільки системний адміністратор та адміністратор безпеки.

Експлуатаційна документація на АІС ЦБД ПН містить опис протоколів, які описують стандартні операційні процедури відновлення інформації з резервних копій та повноваження системного адміністратора та адміністратора

безпеки щодо відновлення інформації, та стандартні операційні процедури повернення АІС ЦБД ПН до режиму цілодобового функціонування.

4.6.4.9 Специфікації послуги "Захищений журнал (НР-2)"

Політика реєстрації повинна стосуватись наступних дій користувачів АІС ЦБД ПН:

– створення бази даних, створення/модифікація/видалення таблиць та структури бази даних;
– доступ до об'єктів захисту АІС ЦБД ПН та дії з ними;
– підключення/відключення до/від бази даних;
– внесення змін до таблиць бази даних (додавання/зміна/видалення записів в таблицях бази даних);
– здійснення резервного копіювання таблиць бази даних;
– вхід/вихід користувачів до АІС ЦБД ПН;
– створення/модифікація/видалення користувачів в АІС ЦБД ПН;
– управління правами користувачів АІС ЦБД ПН;
– помилки, що виникають під час функціонування АІС ЦБД ПН.

Журнал реєстрації містить інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Інформація, включена до журналу реєстрації, є достатньою для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. Конкретний перелік подій, що реєструються, а також параметрів, які характеризують ці події, уточняються на етапі проектування КСЗІ в АІС ЦБД ПН.

Системний адміністратор повинен мати засоби перегляду журналів реєстрації, що ведуться засобами системного програмного забезпечення (операційних систем) та технічними засобами телекомунікацій.

Адміністратор безпеки повинен мати засоби перегляду журналів реєстрації, що ведуться засобами системного програмного забезпечення (операційних систем), системи керування базами даних (СКБД), прикладного програмного забезпечення, технічними засобами телекомунікацій та обладнанням мережевої безпеки.

КЗЗ повинен забезпечувати захист журналів реєстрації від несанкціонованого доступу, модифікації або руйнування.

4.6.4.10 Специфікації послуги "Одиночна ідентифікація та автентифікація (НИ-2)"

Політика одиночної ідентифікації і автентифікації, що реалізується КЗЗ, повинна відноситись до всіх користувачів, наведених в таблиці 4.3, та визначати атрибути, які використовують ці користувачі з числа, перелічених в п. 4.1.7 ТЗ. Кожний користувач з наведеного переліку повинен однозначно ідентифікуватися КЗЗ.

Користувачі повинні ідентифікуватись та автентифікуватись:

– засобами системного програмного забезпечення АІС ЦБД ПН – користувачі [А_СА], [А_АБ], [А_АВ];
– засобами системного та/або прикладного програмного забезпечення АІС ЦБД ПН – користувачі [А_АБ], [О_У], [О_Т], [О_К].

Перш ніж дозволити користувачам виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен ідентифікувати та автентифікувати цих користувачів.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

4.6.4.11 Специфікації послуги "Однонаправлений достовірний канал (НК-1)"

Політика достовірного каналу стосується всіх користувачів, наведених в таблиці 4.3.

Для встановлення достовірного каналу повинні використовуватись штатні засоби системного та прикладного програмного забезпечення, а також комутаційного обладнання АІС ЦБД ПН.

Кожний раз при формуванні достовірного каналу користувач шляхом візуального аналізу зовнішнього вигляду форми для введення атрибутів доступу (ідентифікатора, пароля тощо), що належить операційній системі, СКБД або відповідному додатку, повинен пересвідчитись, що він взаємодіє безпосередньо із відповідним програмним забезпеченням АІС ЦБД ПН. В разі, якщо користувачем виявлено підозру щодо належності цієї форми до відповідних ресурсів АІС ЦБД ПН, формування достовірного каналу ним повинно бути припинено.

4.6.4.12 Специфікації послуги "Розподіл обов'язків адміністраторів (НО-3)"

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати множину ролей адміністраторів та ролей користувачів.

Політика розподілу обов'язків, що застосовується в межах АІС ЦБД ПН, повинна визначати ролі адміністраторів (адміністратор безпеки, системний адміністратор, віддалений адміністратор) та роль користувачів. Обов'язки наведених посадових осіб наведені в п. 3.7.1 ТЗ.

Системний адміністратор має адміністративні права в операційних системах технічних засобів АІС ЦБД ПН та, відповідно, повний доступ до технологічної інформації, що на них обробляється. Адміністратор безпеки має адміністративні права в операційних системах та СКБД. Віддалений адміністратор має обмежені права, що дозволяють лише керувати налаштуваннями прикладного програмного забезпечення АІС ЦБД ПН. Користувачі мають обмежені облікові записи в системному та прикладному програмному забезпеченні, що дозволяють їм виконувати дії лише в рамках власних повноважень.

Управління правами користувачів щодо доступу до інформації, яка обробляється та зберігається в АІС ЦБД ПН, здійснюється адміністратором безпеки.

Відповідний користувач повинен виступати в певній ролі тільки після того, як КЗЗ виконав процедури його автентифікації та авторизації, використовуючи при цьому атрибути, наведені в п. 4.1.7 ТЗ. Користувач, який

успішно пройшов автентифікацію та авторизацію, може виконувати тільки дії, що дозволені для його облікового запису (ролі).

4.6.4.13 Специфікації послуги "КЗЗ з контролем цілісності (НЦ-1)"

Політика цілісності КЗЗ повинна визначати склад КЗЗ. До складу КЗЗ повинні бути включені всі програмні та технічні засоби, функції яких використовуються в реалізації політики безпеки. На етапі проектування КСЗІ в АІС ЦБД ПН повинні бути описані механізми контролю цілісності компонентів, що входять до складу КЗЗ. В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити системного адміністратора та адміністратора безпеки і перевести АІС ЦБД ПН до стану, з якого повернути її до нормального функціонування можуть тільки ці адміністратори.

На етапі проектування КСЗІ в АІС ЦБД ПН повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ АІС ЦБД ПН і всі запити на доступ до захищених об'єктів контролюються цим КЗЗ.

Під час оновлення програмного забезпечення має бути автентифіковано джерело оновлення та перевірено цілісність оновлення.

4.6.4.14 Специфікації послуги "Самотестування при старті (НТ-2)"

Політика самотестування, що реалізується КЗЗ, повинна відноситися до програмних та технічних засобів, функції яких використовуються в реалізації політики безпеки. На етапі проектування КСЗІ в АІС ЦБД ПН повинні бути визначені та описані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за відповідним запитом системного адміністратора або адміністратора безпеки, а також при ініціалізації засобів захисту інформації зі складу КЗЗ.

4.6.4.15 Специфікації послуги "Автентифікація вузлу (НВ-1)"

Політика ідентифікації та автентифікації при обміні, яка реалізується КЗЗ, повинна відноситись до процедур встановлення захищеного з'єднання через мережу Інтернет між:

– ОЦОД та РЦОД АІС ЦБД ПН;
– АІС ЦБД ПН та операторами телекомунікацій;
– АІС ЦБД ПН та ІТС операторів телекомунікацій, державних органів, суб'єктів господарювання;
– ОЦОД (РЦОД) та робочим місцем віддаленого адміністрування.

При встановленні захищеного з'єднання КЗЗ повинен забезпечувати автентифікацію сторін обміну даними, між якими встановлюється захищене з'єднання. Якщо процедуру проведення автентифікації завершено невдало, захищене з'єднання не повинно бути встановлено.

Атрибутами автентифікації КЗЗ є ключові пари (особисті та відкриті ключі), що використовуються в засобах криптографічного захисту інформації, які застосовуються в складі КЗЗ компонент АІС ЦБД ПН для захисту інформації, що передається між ними.

Додатково автентифікація операторів телекомунікацій здійснюється за електронним підписом на запитах/відповідях, обмін якими здійснюється в процесі функціонування АІС ЦБД ПН (п. 3.5.4 ТЗ).

Для реалізації послуги повинні використовуватись програмні засоби криптографічного захисту інформації, які мають позитивні експертні висновки в сфері криптографічного захисту інформації.

Під час оновлення програмного забезпечення має бути автентифіковано джерело оновлення та перевірено цілісність оновлення.

4.7 Вимоги до рівня гарантій

Послуги безпеки КСЗІ в АІС ЦБД ПН повинні бути реалізовані з рівнем гарантій Г-2 згідно з НД ТЗІ 2.5-004-99. Специфікації всіх критеріїв гарантій повинні в повному обсязі відповідати НД ТЗІ 2.5-004-99.

4.8 Вимоги до КСЗІ в частині захисту від витоку інформації технічними каналами

Вимоги до КСЗІ АІС ЦБД ПН в частині захисту від витоку інформації технічними каналами не висуваються.

4.9 Вимоги до системи електроживлення

Для забезпечення працездатності технічні засоби ОЦОД та РЦОД повинні бути обладнані джерелами безперебійного живлення. Потужність джерел безперебійного живлення має бути достатньою для коректного завершення роботи компонентів АІС ЦБД ПН, окремого пристрою або відновлення їх працездатності.

5 ВИМОГИ ДО ДОКУМЕНТАЦІЇ

5.1 Склад документації на КСЗІ

Документація на КСЗІ в АІС ЦБД ПН повинна складатись з:
- передпроектних робіт;
- проектної;
- нормативно-розпорядчої;
- щодо проведених випробувань КСЗІ;
- організаційно-розпорядчої;
- супровідної.

5.1.1 Документація етапу передпроектних робіт

Документація етапу передпроектних робіт повинна включати:
- положення про службу захисту інформації в АІС ЦБД ПН;
- акт обстеження середовищ функціонування АІС ЦБД ПН;
- акт категоріювання АІС ЦБД ПН;
- політика безпеки інформації в АІС ЦБД ПН;
- модель порушника безпеки інформації в АІС ЦБД ПН;
- модель загроз для інформації в АІС ЦБД ПН;
- план захисту інформації в АІС ЦБД ПН;
- технічне завдання на створення КСЗІ.

5.1.2 Проектна документація на КСЗІ

Проектна документація на КСЗІ відповідно до НД ТЗІ 3.7-003-2005 повинна включати:
- ескізного проекту КСЗІ (у разі проведення ескізного проектування);
- технічного проекту КСЗІ;
- робочого проекту КСЗІ.

5.1.3 Нормативно-розпорядча документація КСЗІ

Нормативно-розпорядча документація КСЗІ повинна включати:
- посадові (функціональні) інструкції працівників СЗІ, користувачів АІС ЦБД ПН:
- інструкції адміністраторів АІС ЦБД ПН;
- інструкція користувача АІС ЦБД ПН;
- технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ:
  - порядок модернізації та оновлення компонентів АІС ЦБД ПН;
  - порядок оперативного відновлення функціонування АІС ЦБД ПН;
  - інструкція з організації контролю за функціонуванням КСЗІ;
  - інструкції про порядок використання засобів КЗІ.

5.1.4 Документація щодо випробувань КСЗІ

Документація щодо випробувань КСЗІ відповідно до НД ТЗІ 3.7-003-2005 повинна включати:

– програма та методика попередніх випробувань КСЗІ в АІС ЦБД ПН;
– протокол попередніх випробувань КСЗІ в АІС ЦБД ПН.

5.1.5 Організаційно-розпорядча документація КСЗІ

Організаційно-розпорядча документація КСЗІ відповідно до НД ТЗІ 3.7-003-2005 повинна включати:

– акт про приймання КСЗІ АІС ЦБД ПН у дослідну експлуатацію;
– акт завершення дослідної експлуатації КСЗІ АІС ЦБД ПН;
– акт завершення робіт зі створення КСЗІ АІС ЦБД ПН.

Додатково організаційно-розпорядча документація КСЗІ повинна включати:

– проект наказу замовника про призначення служби захисту інформації;
– проект наказу замовника про призначення комісії для проведення обстеження середовищ функціонування АІС ЦБД ПН та категоріювання об'єкту інформаційної діяльності;
– проект наказу замовника про призначення комісії для проведення попередніх випробувань КСЗІ АІС ЦБД ПН;
– проект наказу замовника про створення комісії для приймання КСЗІ в дослідну експлуатацію.

5.1.6 Супровідна документація КСЗІ

Супровідна документація КСЗІ відповідно до НД ТЗІ 3.7-003-2005 повинна включати:

– формуляр АІС ЦБД ПН;
– реєстраційні журнали, використовувані для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

Остаточний склад документації, що розробляється, уточнюється на етапі розробки КСЗІ в АІС ЦБД ПН та узгоджується з замовником.

6 ЕТАПИ ВИКОНАННЯ РОБІТ

Етапи виконання робіт з розробки КСЗІ наведені в таблиці 6.1.

Таблиця 6.1 – Етапи виконання робіт з розробки КСЗІ

Етапи	Зміст робіт
1 Обстеження середовищ функціонування АІС ЦБД ПН та розроблення ТЗ на КСЗІ	1.1 Обстеження середовищ функціонування АІС ЦБД ПН. 1.2 Категоріювання об'єкту інформаційної діяльності. 1.3 Розробка документації передпроектних робіт. 1.4 Розроблення та погодження ТЗ на КСЗІ.
2 Проектування КСЗІ	2.1 Проектування КСЗІ. 2.2 Розроблення проектної документації КСЗІ. 2.3 Розроблення експлуатаційної документації КСЗІ. 2.4 Розробка плану захисту інформації. 2.5 Налаштування КЗЗ.
3 Попередні випробування КСЗІ	3.1 Розроблення програми та методики попередніх випробувань КСЗІ. 3.2 Проведення попередніх випробувань КСЗІ. 3.3 Оформлення результатів попередніх випробувань та акта про прийняття КСЗІ до дослідної експлуатації.
4 Дослідна експлуатація КСЗІ	4.1 Підготовка користувачів. 4.2 Пусконалагоджувальні роботи. 4.3 Проведення дослідної експлуатації, доопрацювання складових частин КСЗІ та корегування робочої документації за результатами дослідної експлуатації.
5 Державна експертиза КСЗІ	5.1 Подача заявки на проведення державної експертизи КСЗІ. 5.2 Визначення організатора експертизи для проведення експертних досліджень КСЗІ. 5.3 Проведення експертних досліджень КСЗІ та надання атестату відповідності.

Примітка. Роботи за пунктом 5.3 проводяться експертним закладом (експертами), визначеним організатором експертизи, у встановленому порядку в строки, передбачені відповідними господарськими договорами.

Допускається виконувати окремі етапи робіт до завершення попередніх етапів, паралельне у часі виконання етапів робіт, додавання нових етапів робіт.

7 ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ

Об'єктом випробувань є КСЗІ в АІС ЦБД ПН.

Метою випробувань є встановлення відповідності досягнутого в КСЗІ в АІС ЦБД ПН рівня захищеності інформації вимогам ТЗ та визначення її готовності до експлуатації.

Передбачається проведення таких видів випробувань: попередні випробування, дослідна експлуатація, державна експертиза КСЗІ. Для кожного виду випробувань виконавцем повинна бути розроблена та затверджена у встановленому порядку відповідна програма та методика випробувань. Обсяг випробувань повинен забезпечити вичерпну оцінку усіх показників захисту інформації.

Методи проведення попередніх випробувань мають бути орієнтовані на подальшу експертну оцінку впроваджених в АІС ЦБД ПН засобів захисту інформації при проведенні державної експертизи КСЗІ.

Випробування проводяться за умови наявності усієї сукупності апаратних та програмних засобів захисту інформації, а також технічної документації на КСЗІ, що розробляється згідно з вимогами ТЗ.

Для проведення попередніх випробувань та дослідної експлуатації призначається комісія.

При проведенні попередніх випробувань та дослідної експлуатації КСЗІ забороняється обробка в АІС ЦБД ПН інформації, що підлягає захисту.

За результатами попередніх випробувань КСЗІ, усунення недоліків (у випадку їх наявності) та коригування проектної, експлуатаційної документації оформлюється акт про приймання КСЗІ в дослідну експлуатацію.

За результатами дослідної експлуатації КСЗІ, усунення недоліків (у випадку їх наявності) та коригування проектної, експлуатаційної документації оформлюється акт про завершення дослідної експлуатації, який повинен містити висновки щодо можливості представлення КСЗІ для проведення державної експертизи в сфері ТЗІ.

Державна експертиза КСЗІ в АІС ЦБД ПН здійснюється відповідно до Положення про державну експертизу в сфері технічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку України від 16 травня 2007 р. № 93.

8 ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОНАННІ РОБІТ

Перелік осіб, які можуть бути ознайомлені з матеріалами проектної та експлуатаційної документації на КСЗІ в АІС ЦБД ПН, що містять інформацію з обмеженим доступом, затверджується керівництвом ДП "Український державний центр радіочастот".

Порядок доступу таких осіб до зазначених матеріалів встановлюється згідно з нормативними документами України.

9 ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЗ

Зміни та доповнення до ТЗ на створення КСЗІ оформлюються окремими доповненнями, які погоджуються та затверджуються у порядку, встановленому для основного ТЗ.

Доповнення до ТЗ на КСЗІ складається з вступної та змістовної частин. У вступній частині зазначається причина випуску доповнення. В змістовній частині наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

Начальник відділу проведення
державних експертиз
ТОВ "ІНТЕСИС"

_____ О.В. Шеметов

"08" 04 2019 р.

Заступник начальника відділу захисту
інформації департаменту ІТ
ДП "Український державний центр
радіочастот"

_____ В.І. Бондаренко

"08" 04 2019 р.