ДЕРЖАВНА СЛУЖБА СТАТИСТИКИ УКРАЇНИ

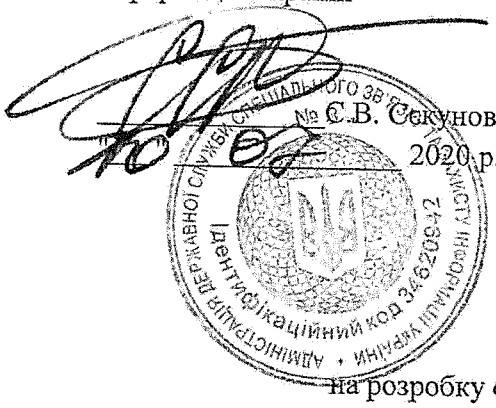
Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі:

Послуги з упровадження комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційній системі (ІТС) органів державної статистики (ОДС) (обласний рівень) (код відповідно до національного класифікатора України ДК 021:2015 "Єдиний закупівельний словник": 72590000-7 Професійні послуги у комп'ютерній сфері)

Київ – 2021

Прим. № 1

ПОГОДЖЕНО
Перший заступник Голови
Державної служби
спеціального зв'язку та захисту
інформації України



_____ С.В. Секунов
"___" _____ 2020 р.

ЗАТВЕРДЖЕНО
Генеральний директор
АТ "ІІТ"

_____ В.В. Онопріенко
"___" _____ 2020 р.

ЗАТВЕРЖЕНО
Голова Державної служби
статистики України

_____ І.Є. Вернер
"___" _____ 2020 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на розробку організаційно-технічного рішення на розгортання
типової складової компоненти комплексної системи захисту інформації
в інформаційно-телекомунікаційній системі
органів державної статистики України
(обласний рівень)
нова редакція на заміну ЄААД.468244.276 ТЗ.02

Шифр "КСЗІ ІТС ОДС ОР"

ЄААД.468244.276 ТЗ.02.1

2020

90 Вх 3434 90-Вх-252-1-4

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АПЗ	–	Апаратно-програмний засіб
АРМ	–	Автоматизоване робоче місце
БД	–	База даних
ГУС	–	Головне управління статистики
ДССУ	–	Державна служба статистики України
ДСТУ	–	Державний стандарт України
ЕОМ	–	Електронна обчислювальна машина
КЕП	–	Кваліфікований електронний підпис
ЄДРПОУ	–	Єдиний державний реєстр підприємств та організацій України
ІССІ	–	Інтегрована система статистичної інформації
ІТС	–	Інформаційно-телекомунікаційна система
КЕОІ	–	Комплекс електронної обробки інформації
КЗЗ	–	Комплекс засобів захисту
КЗІ	–	Криптографічний захист інформації
КМУ	–	Кабінет Міністрів України
КНЕДП	–	Кваліфікований надавач електронних довірчих послуг
КСЗІ	–	Комплексна система захисту інформації
КТЗ	–	Комплекс технічних засобів
ЛОМ	–	Локальна обчислювальна мережа
НД	–	Нормативний документ
НКІ	–	Носій ключової інформації
НСД	–	Несанкціонований доступ
ОДС	–	Орган державної статистики
ОР	–	Обласний рівень
ОС	–	Операційна система
ПЗ	–	Програмний засіб
ПК	–	Програмний комплекс
РМ	–	Робоче місце
РС	–	Робоча станція
СЕДО	–	Система електронного документообігу
СКБД	–	Система керування базами даних
ТЗ	–	Технічне завдання
ТЗІ	–	Технічний захист інформації
ТІ	–	Технологічна інформація
ФПЗ	–	Функціональний профіль захисту
ФС	–	Файлова система
ЦР	–	Центральний рівень
ЦСК	–	Центр сертифікації ключів
IP	–	Internet Protocol
VPN	–	VirtualPrivateNetwork

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому технічному завданні (далі – ТЗ) застосовуються терміни і визначення, які відповідають встановленим ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни й визначення" і НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Повне найменування КСЗІ та її умовне позначення

Організаційно-технічне рішення на розгортання типової складової компоненти комплексної системи захисту інформації (далі – КСЗІ) в інформаційно-телекомунікаційній системі органів державної статистики України (обласний рівень) (далі – ІТС ОДС ОР).

1.2 Шифр теми

Шифр КСЗІ: "КСЗІ ІТС ОДС ОР".

1.3 Відомості про замовника і розробника ТЗ на КСЗІ

Замовник ОТР КСЗІ та власник ІТС – Державна служба статистики України (далі – Держстат). Юридична адреса:01601, м. Київ, вул. Ш. Руставелі, 3.

Розробник ТЗ – Приватне акціонерне товариство "Інститут інформаційних технологій" (далі – АТ "ІІТ"). Юридична адреса: 61166, м. Харків, вул. Бакуліна, 12. Тел./факс: (057) 714-22-05.

1.4 Перелік документів, на підставі яких створюється ТЗ на ОТР КСЗІ, ким і коли затверджені ці документи

Розробка нової редакції ТЗ на ОТР КСЗІ в ІТС ОДС ОР на заміну "ЄААД.468244.276 ТЗ.02 Технічне завдання на розробку організаційно-технічного рішення на розгортання типової складової компоненти комплексної системи захисту інформації в інформаційно-телекомунікаційній системі органів державної статистики України (обласний рівень)" виконується за договором № 47 від 01.04.2020 між Держстатом та АТ "ІІТ".

Попередня редакція "ЄААД.468244.276 ТЗ.02 Технічне завдання на розробку організаційно-технічного рішення на розгортання типової складової компоненти комплексної системи захисту інформації в інформаційно-телекомунікаційній системі органів державної статистики України (обласний рівень)" погоджена Адміністрацією Держспецзв'язку вих. Адміністрації Держспецзв'язку від 13.12.2018 №04/01/02-4833.

1.5 Планові терміни початку й закінчення роботи зі створення КСЗІ

Мають бути визначенні відомістю виконання робіт, що є невід'ємним додатком до договору зі створення ОТР КСЗІ.

1.6 Відомості про джерела й порядок фінансування робіт

Фінансування робіт з розробки нової редакції ТЗ на ОТР КСЗІ в ІТС ОДС ОР виконується за договором № 47 від 01.04.2020 між Держстатом та АТ "ІІТ".

1.7 Порядок подання результатів робіт

Порядок оформлення та подання результатів роботи зі створення ОТР КСЗІ в ІТС ОДС ОР повинен відповідати вимогам РД 50-34.698-90, ДСТУ 3396.1-96, НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-001-99 та НД ТЗІ 3.7-003-05.

2 МЕТА Й ПРИЗНАЧЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Мета створення КСЗІ

Організаційно-технічне рішення створюється з метою оцінки сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації ІТС ОДС ОР, при впровадженні на реальному об'єкті утворюють КСЗІ ІТС ОДС ОР.

Метою створення КСЗІ є забезпечення захисту інформації, що циркулює в ІТС ОДС ОР. Захист інформації має здійснюватися шляхом протидії загрозам, які можна очікувати внаслідок дій порушника на всіх технологічних етапах її обробки і в усіх режимах функціонування ІТС ОДС ОР.

При розробці ОТР КСЗІ повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного захисту інформації (далі – ТЗІ).

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІТС ОДС ОР у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

– організаційно-правові заходи, які реалізуються поза обчислювальною системою ІТС ОДС ОР;

– інженерно-технічні заходи, що реалізуються поза обчислювальною системою ІТС ОДС ОР;

– апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу, реалізації функцій криптографічного захисту інформації (далі – КЗІ) та забезпечення доступності інформації, яка обробляється й зберігається у ІТС ОДС ОР.

2.2 Функціональне призначення ОТР КСЗІ

Організаційно-технічне рішення призначене для:

– реалізації політики безпеки інформації заданої в ІТС ОДС ОР;

– ідентифікації та автентифікації користувачів у ході надання їм доступу до функцій та інформації ІТС ОДС;

– забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в ІТС ОДС ОР;

– розмежування доступу користувачів до інформації та функцій ІТС ОДС ОР;

– забезпечення конфіденційності та цілісності технологічної інформації, що обробляється та передається каналами зв'язку у ІТС ОДС ОР;

– реалізації функцій криптографічного захисту інформації (далі – КЗІ), що передається каналами зв'язку між компонентами ІТС ОДС ОР та іншими елементами, що беруть участь в обробці інформації ІТС;

– створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації;

– ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи ІТС ОДС ОР, причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;

– забезпечення захисту обчислювальних ресурсів та компонентів ІТС ОДС ОР з боку мережі Інтернет (в тому числі унеможливлення попадання шкідливого ПЗ та запобігання від НСД до ІТС);

– керування засобами захисту інформації, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації у ІТС ОДС ОР;

– 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 ІТС ОДС ОР;

– реєстрації, збору, зберігання, обробки даних про події у ІТС ОДС ОР, які мають відношення до безпеки інформації;

– забезпечення доступності ресурсів ІТС ОДС ОР для її користувачів.

2.3 Нормативно-правові акти та нормативні документи, що є основою для створення ОТР КСЗІ

ОТР КСЗІ має розроблятися із врахуванням вимог:

– Закону України "Про державну статистику";

– Закону України "Про доступ до публічної інформації";

– Закону України "Про електронні довірчі послуги";

– Закону України "Про електронні документи та електронний документообіг";

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

– Закону України "Про захист персональних даних";

– Закону України "Про інформацію";

– Постанови КМУ "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 р. № 373;

– Постанови КМУ "Про створення Єдиного державного реєстру підприємств та організацій України" від 22.01.1996 р. № 118;

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

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

– 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 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу;

– НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

3 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІТС ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ

3.1 Загальна характеристика ІТС

ІТС ОДС складається з двох рівнів:

- ІТС ОДС центрального рівня (далі – ІТС ОДС ЦР);
- ІТС ОДС ОР.

Створення КСЗІ в ІТС ОДС ЦР визначено окремим технічним завданням.

ІТС ОДС ОР є багатомашинним багатокористувачевим комплексом, до складу якого входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі, технологія її оброблення.

До складу ІТС ОДС ОР входять наступні підсистеми:

- система Єдиного державного реєстру підприємств та організацій України (далі – ЄДРПОУ);
- інтегрована система статистичної інформації (далі – ІССІ);
- система електронного документообігу (далі – СЕДО) ОДС;
- система електронної звітності (далі – СЕЗ);
- інші корпоративні сервіси ОДС ЦР (далі – КС).

Згідно НД ТЗІ 2.5-005-99 ІТС ОДС ЦР класифікується як автоматизована система (далі – АС) класу "3".

3.2 Основні функціональні завдання

В процесі свого функціонування ІТС ОДС ОР забезпечує виконання наступних задач:

- забезпечення обробки, відправлення, одержання, зберігання інформації у вигляді електронних документів в ІТС ОДС ОР у взаємодії з центральним рівнем;
- забезпечення інформаційної взаємодії структурних підрозділів ОДС ОР та інших територіальних підрозділів;
- скорочення строків опрацювання документів та інформації у структурних підрозділах ОДС ОР;
- забезпечення організації працівників ІТС ОДС ОР корпоративними сервісами;
- видача довідок з ЄДРПОУ;
- отримання даних ЄДРПОУ з ІТС ОДС ЦР;
- забезпечення конфіденційності та цілісності інформації, яка обробляється в ІТС ОДС ОР, та забезпечення її доступності для користувачів системи;
- приймання статистичної інформації на території регіону;
- введення інформації в комплекс електронної обробки статистичної інформації (далі – КЕОІ);
- обробку статистичної інформації відповідно до чинного законодавства України та задач, які ставляться керівництвом Держстату;
- керування доступом до інформації, яка обробляється в ІТС ОДС ОР;
- підготовка звітів та результатів статистичних досліджень;

– забезпечення можливості розміщення результатів статистичних досліджень на офіційних веб-ресурсах Держстату;
– контроль паперових звітів;
– реєстрація та аудит подій в системі та контроль за діями користувачів ІТС ОДС ОР;
– зв'язок з ІТС ОДС ЦР.

3.3 Комплекс технічних засобів

До складу комплексу технічних засобів (далі – КТЗ) обчислювальної системи ІТС ОДС ОР відноситься:

– проксі сервер та програмний міжмережевий екран (далі – МЕ) (в подальшому може бути замінений на апаратний МЕ);
– контролери домену;
– файлові сервери;
– сервери підсистеми збирання, обробки, аналізу та поширення статистичної інформації;
– сервери та РС підсистеми "Єдине вікно";
– РС адміністраторів;
– РС внутрішніх користувачів;
– IP-шифратор;
– носій ключової інформації (опціонально);
– багатофункціональні пристрої та принтери;
– джерела безперебійного живлення;
– комунікаційне обладнання.

Проксі сервер та сервер з програмним МЕ призначені для захисту інформаційних ресурсів та інфраструктурних компонентів ІТС ОДС ОР від мережевих атак та зловмисного ПЗ. В подальшому дані компоненти можуть бути перенесені на апаратний МЕ. В такому випадку у якості МЕ повинен використовуватись технічний засіб, що має позитивний експертний висновок Держспецзв'язку у сфері ТЗІ, а перелік покладених функцій може бути розширений.

Контролери домену призначено для централізованого керування обліковими записами користувачів операційних систем серверів (з ОС Microsoft Windows) зі складу ІТС ОДС ОР, РС адміністраторів та РС користувачів, а також для керування обліковими записами та атрибутами доступу користувачів до ресурсів ІТС ОДС ОР. Центральний домен розташовується у складі ІТС ОДС ЦР, а контролер домену у складі ІТС ОДС ОР з ним реплікується і забезпечує керування обліковими записами в межах регіону. Крім того в ІТС ОДС ОР розгорнуто додаткові домени у виокремлених мережах для спрощення управлянні обліковими записами в цих мережах.

Файлові сервери призначені для доступу до файлів за протоколом SMB. Файлові сервери необхідні для обміну файлами у корпоративній мережі ІТС ОДС ОР, а також з ІТС ОДС ЦР.

Підсистема збирання, обробки, аналізу та поширення статистичної інформації, що функціонує на базі інтегрованої системи статистичної інформації (далі – ІССІ) та КЕОІ складається з наступних серверів:

- Головний сервер БД ІССІ;
- Сервер застосувань тестового середовища ІССІ;
- Головний сервер БД тестового середовища ІССІ;
- Сервер застосувань (EAS/IIS) ІССІ;
- Сервер реплікації ІССІ;
- Сервер БД ІССІ.

В корпоративній мережі на окремому сервері знаходиться серверна частина підсистеми "Єдине вікно" (є власною розробкою для всіх ІТС ОДС ОР). Основні призначення даної підсистеми – реєстрація звітів, що були надані респондентами. Вміст звітів в даній підсистемі не обробляється. Відповідні РС цієї підсистеми призначені для наповнення її БД.

РС використовуються адміністраторами та користувачами для виконання функціональних завдань в ІТС ОДС ОР.РС можуть використовуватися користувачами ІТС ОДС ОР для виконання різних функціональних завдань, що передбачають різну технологію роботи (детально описано в п. 3.9). В цьому випадку РС для різних задач можуть визначатись окремі або за наявності необхідних фізичних ресурсів кожна РС може використовуватись для різних технологічних завдань ІТС ОДС ОР. РС користувачів взаємодіє з ІТС ОДС ЦР через мережу Держстату.

НКІ, це пристрої, що призначені для збереження особистих ключів користувачів та адміністраторів, які використовуються в СЕДО, для накладання та перевірки КЕП, а також для підвищення рівня захисту особистих ключів. У якості НКІ мають використовуватись апаратно-програмні засоби КЗІ (далі – АПЗ КЗІ), що мають позитивні експертні висновки Держспецзв'язку у сфері КЗІ.

IP-шифратор призначений для встановлення захищених з'єднань між ІТС ОДС ОР та IP-шифраторами зі складу ІТС ОДС ЦР, що дозволяє шифрувати та контролювати цілісність IP-пакетів між цими ІТС.

Джерела безперебійного живлення (автоматичні пристрої електроживлення) призначені для забезпечення безперебійного постачання електричною енергією компонентів ІТС в межах норми (у випадках стрибків напруги або повного відключення електроенергії).

Комунікаційне обладнання – мережеві керовані пристрої (активне мережеве обладнання), що призначені для забезпечення обміну інформацією між компонентами ІТС ОДС ОР та взаємодією з мережею Інтернет та територіальними підрозділами статистики.

Комунікаційне обладнання Спільного українсько-німецького підприємства "Інфоком" підключається до комутаторів і забезпечує для ІТС ОДС ОР доступ в мережу Держстату та мережу Інтернет.

Структурна схема КТЗ ІТС ОДС ОР наведена на рис. 3.1.

В процесі технічного проектування може бути прийнято рішення щодо переміщення частини компонентів ІТС ОДС ОР у віртуальне середовище, а склад засобів може бути уточнений.

До складу ІТС ОДС ОР не входять, але взаємодіють із нею:

- ІТС ОДС ЦР;
- спільне українсько-німецьке підприємство ТОВ "Інфоком" (далі – провайдер);
- кваліфіковані надавачі електронних довірчих послуг (далі – КНЕДП).

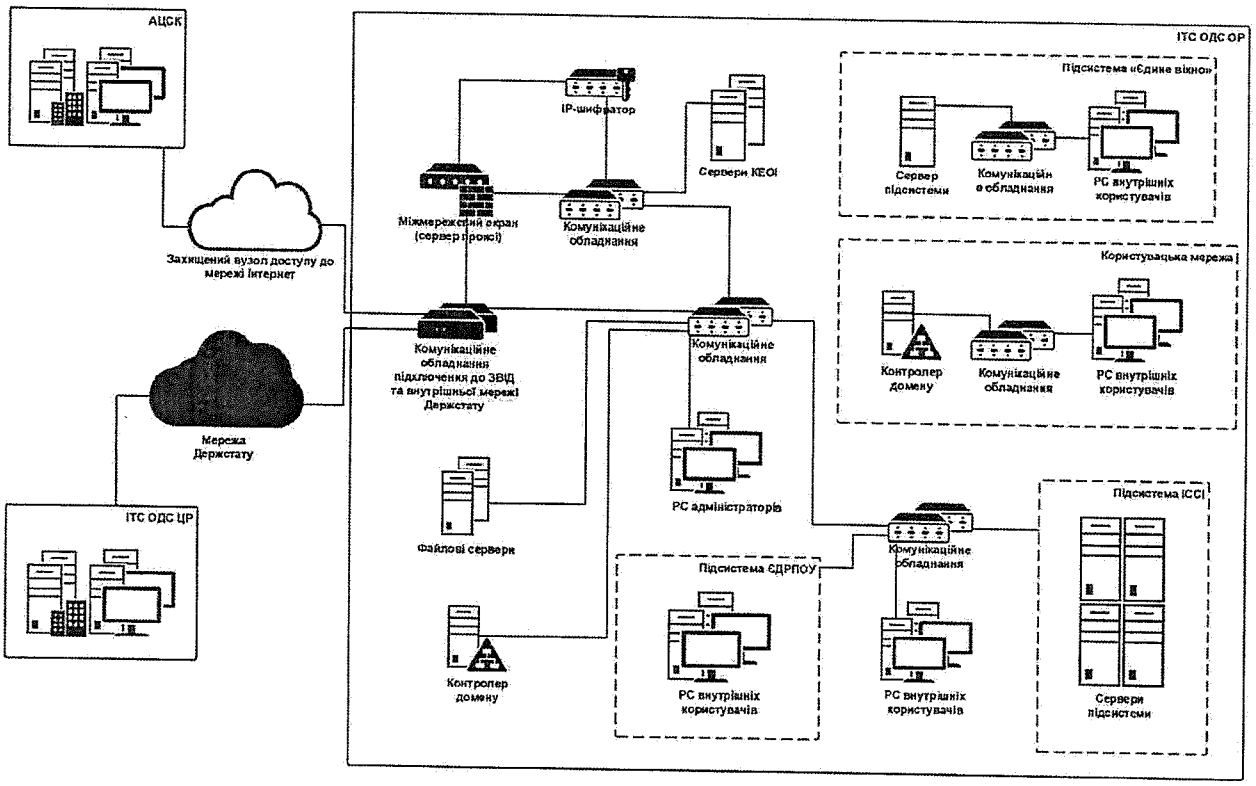


Рисунок 3.1 – Структурна схема КТЗ ІТС ОДС ОР

3.4 Програмне забезпечення

Програмне забезпечення (далі – ПЗ) ІТС ОДС ОР складається з системного та функціонального ПЗ. До програмного забезпечення ІТС ОДС ОР відноситься:

- операційна система серверів – Microsoft Windows Server 2008 R2 (або вище), Centos 6 (або вище);
- операційні системи РС – Microsoft Windows 7 Professional/Enterprise (або вище);
- система керування базами даних (далі – СКБД) – Oracle Database 11 (або вище), FoxPro, Sybase та відповідні клієнти;
- ПЗ антивірусного захисту з ПЗ керування – ESET Endpoint Antivirus 5 (або вище);
- ПК віддаленого управління IP-шифратором;
- Функціональне програмне забезпечення (далі – ФПЗ) ІССІ – програмне забезпечення власного виробництва;
- ФПЗ для проведення статистичних досліджень і обробки статистичної інформації: Clipper, Power Builder тощо (у складі підсистеми КЕОІ);

– ПЗ міжмережевого екрану та проксі-з'єднань – pfSense;
– загальне програмне забезпечення – Microsoft Office, веб-браузери, поштові клієнти, прикладне програмне забезпечення для проведення статистичних досліджень та інше.

Системне ПЗ ІТС ОДС ОР повинне забезпечувати виконання наступних основних функцій:

– колективну роботу користувачів;
– адміністрування компонентів ІТС ОДС ОР;
– збереження структурованої і неструктурованої інформації ІТС ОДС ОР;
– доступ до файлів, баз даних і електронних документів колективного користування ІТС ОДС ОР.

ОС робочих станцій призначена для управління ресурсами РС та організації взаємодії з користувачем, а також для забезпечення загальносистемного функціонування іншого ПЗ РС. ОС РС підключається до домену зі складу ІТС ОДС ОР.

СКБД – комплекс програмних застосувань, що забезпечують обробку запитів від користувачів ІТС ОДС ОР на читання або модифікацію інформації, що зберігається в БД. СКБД використовується ФПЗ для виконання основних задач по обробці статистичної інформації в ІТС ОДС ОР.

ФПЗ ІССІ та інше ФПЗ призначено для використання в органах державної статистики і вирішення конкретних завдань введення первинних даних та оброблення статистичної інформації Держстату та інших заходів, результатом проведення/виконання яких є отримання вихідної статистичної інформації. Детальні відомості щодо роботи з ПЗ і відповідно функцій ПЗ наведені в п.3.6.

ПЗ антивірусного захисту – комплекс програмних модулів для виявлення і знешкодження комп'ютерних вірусів і шкідливих програм в режимі реального часу.

ПЗ МЕ та проксі-з'єднань призначені для захисту мережевих компонентів ІТС зі сторони зовнішніх мереж, а також розділення внутрішніх мереж.

ПК віддаленого управління IP-шифратором призначено для здійснення налаштувань IP-шифратора.

Текстові та графічні редактори, а також інше загальне програмне забезпечення, використовуються користувачами для роботи з текстовими та графічними документами при виконанні своїх посадових обов'язків.

Веб-браузер використовується користувачами для доступу до функцій та інформації розміщеної на веб-сайтах.

Поштовий клієнт використовується для обміну поштовими повідомленнями через поштові сервіси ІТС ОДС.

Остаточний склад технічних засобів та програмного забезпечення ІТС ОДС ОР уточняється на етапі техноробочого проектування КСЗІ.

3.5 Канали зв'язку

В ІТС ОДС побудовано корпоративну мережу відповідно до Технічного рішення "Модернізація вузлів доступу корпоративної мережі органів державної статистики України" (згідно з контрактом № 4729/55 від 06.12.2010).

Корпоративна мережа ОДС побудована на базі Національної мультисервісної мережі передачі даних УкрПак, офіційним оператором якої є СП "Інфоком". Вона включає в себе один центральний вузол, розташований у приміщенні Держстату за адресою 01601, м. Київ, вул. Еспланадна, 4-6, та 25 регіональних вузлів в обласних центрах та місті Києві.

Центральний вузол мережі пов'язаний з кожним регіональним вузлом виділеними каналами телекомунікаційного зв'язку по радіальній схемі.

З архітектурної точки зору корпоративна мережа ОДС становить собою віртуальну приватну мережу, розгорнуту на транспортній інфраструктурі мережі УкрПак. Такий підхід дозволяє Держстату зекономити значні кошти, які б інакше знадобилися для побудови власної транспортної мережі. У той же час технології, які використовуються в УкрПак, дозволяють досягти такого ж рівня якості передачі інформації, а також ізоляції і захищеності на транспортному рівні, які б мав Держстат у випадку володіння власною мережею. Додаткова економія коштів досягається за рахунок того, що для Держстату відпадає необхідність тримати в штаті, непрофільних для задач статистики, високооплачуваних спеціалістів з телекомунікації. Тобто дана мережа та обладнання, що задіяне для її реалізації, є власністю і відповідно адмініструються провайдером.

25 регіональних вузлів доступу корпоративної мережі мають можливість обміну інформацією корпоративними каналами передачі даних на швидкості від 10 Мбіт/с, у якості маршрутизатора вузлів використовується маршрутизатор CISCO 2801. При цьому підключення до корпоративної телекомунікаційної мережі здійснюється за технологією УкрПак MPLS. Сам канал доступу переведено на оптику. Типова схема регіонального вузла доступу корпоративної мережі наведена на рис.3.2.

Оператор послуг передачі даних має Атестат відповідності (№ 21532 від 21.05.2020) на КСЗІ ІТС захищеного вузла Інтернет-доступу спільного українсько-німецького підприємства у формі товариства з обмеженою відповідальністю "Інфоком".

В серверному сегменті ІТС ОДС ОР засоби підключено до комутаторів, комутація побудована на витій парі зі швидкістю передачі даних до 1 Гбіт/с. Сервери та комутатори знаходяться в серверних шафах.

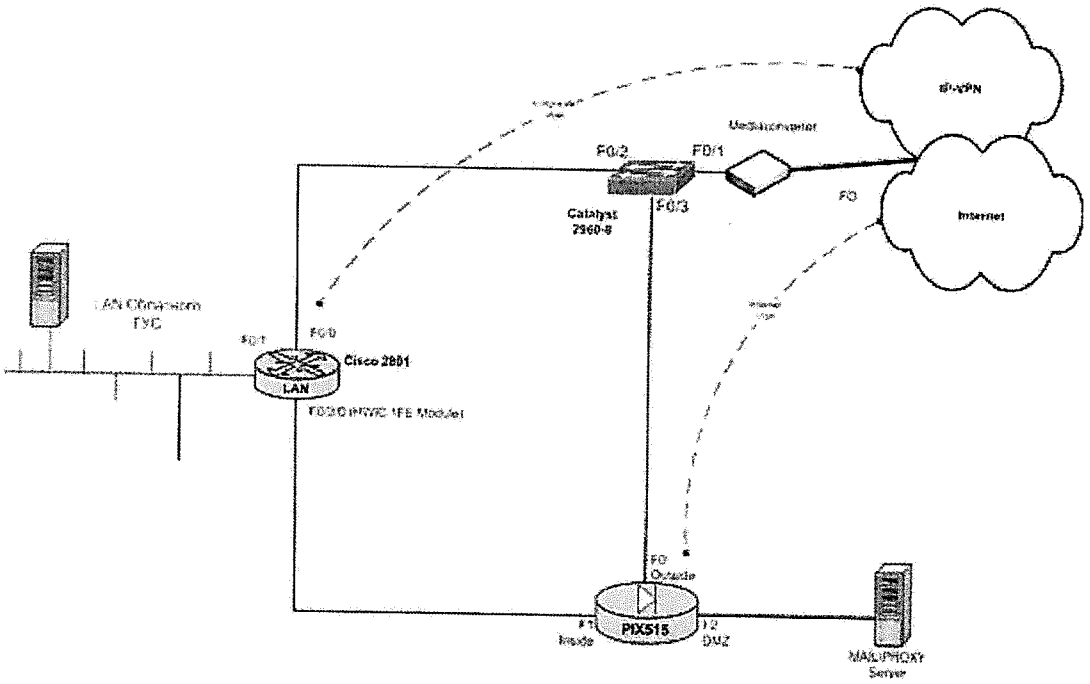


Рисунок 3.2 – Схема регіонального вузла доступу корпоративної мережі

3.6 Характеристика оброблюваної інформації

3.6.1 Категорії інформації

Необхідність захисту інформації, яка обробляється у ІТС ОДС ОР, визначається ст. 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", Постановою КМУ від 29.03.2006 № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" та Законом України "Про державну статистику".

За змістом вимог щодо захисту, оброблювана у ІТС ОДС ОР інформація підрозділяється на такі категорії:

- відкрита інформація;
- конфіденційна інформація;
- технологічна інформація.

3.6.2 Відкрита інформація

До відкритої інформації відносяться статистичні дані (результати обробки та аналізу первинних даних), реєстри, класифікатори, електронні документи, довідники, які обробляється у ІТС, коди ЄДРПОУ. Зазначені дані є державними інформаційними ресурсами, і вимога щодо їх захисту встановлена законом. До інформації цієї категорії висуваються підвищені вимоги із забезпечення цілісності та доступності.

3.6.3 Конфіденційна інформація

До конфіденційної інформації відноситься:

- первинні статистичні дані;

- дані виробничих і фінансово-економічних показників діяльності суб'єктів;
- ідентифікаційні номери фізичних осіб - платників податків;
- особисті ключі КЕП.

Первинні статистичні дані є конфіденційними у відповідності до закону "Про державну статистику".

Джерелами первинної статистичної інформації є звіти, які надаються в Держстат через підсистему звітності, а також звіти, які надаються за результатами їх обробки територіальними підрозділами Держстату та статистичні дані, отримані з АС "Кабінет респондента".

Особисті ключі адміністраторів, користувачів та засобів КЗІ, що будуть використовуватись в ІТС, а також атрибути доступу до ключів повинні бути доступні лише власникам у відповідності до закону "Про електронні довірчі послуги".

До конфіденційної інформації висуваються підвищені вимоги із забезпечення конфіденційності, цілісності та доступності.

3.6.4 Технологічна інформація

Технологічна інформація (далі – ТІ) складається з ТІ комплексу засобів захисту та ТІ щодо адміністрування та управління обчислювальною системою ІТС ОДС ОР. Технологічна інформація призначена для використання тільки уповноваженими адміністраторами з числа персоналу, що забезпечує функціонування ІТС ОДС. До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності та цілісності.

До технологічної відноситься інформація наступного змісту:

- налаштування операційних систем, СКБД, правил розмежування доступу, параметрів безпеки домена;
- налаштування ФПЗ;
- налаштування шлюзу доступу та комунікаційного обладнання;
- налаштування параметрів антивірусного захисту;
- налаштування параметрів взаємодії з СКБД;
- налаштування засобів КЗІ;
- паролів, пін-кодів та інших конфіденційних реквізитів доступу адміністраторів та користувачів ІТС ОДС ОР;
- журнали подій та налаштування щодо фіксації подій у журналах;
- налаштування поштових серверів та внутрішнього веб-сервера.

3.7 Середовище користувачів

3.7.1 Ролі користувачів

Користувачі ІТС ОДС ОР за рівнем повноважень доступу до інформації, що обробляється у ІТС ОДС ОР, характеру й змісту робіт, які виконуються в процесі функціонування, підрозділяються на такі ролі:

- адміністратор безпеки;
- системний адміністратор;

– адміністратор БД;
– внутрішній користувач;

3.7.2 Функції користувачів

3.4.2.1 Основними функціями користувача з роллю "адміністратор безпеки" є:

– організація та контроль якісного виконання організаційно-технічних заходів з захисту інформації в ІТС ОДС ОР;
– адміністрування облікових записів користувачів;
– керування атрибутами доступу користувачів в ІТС ОДС ОР, які використовуються для доступу до ресурсів ІТС ОДС ОР;
– керування журналами реєстрації подій в ІТС ОДС ОР;
– відстеження подій безпеки та реагування на інциденти безпеки ;
– налаштування параметрів безпеки КЗЗ ІТС ОДС ОР;
– контроль параметрів безпеки КЗЗ ІТС ОДС ОР;
– контроль функціонування КЗЗ ІТС ОДС ОР;
– організація забезпечення антивірусного та мережевого захисту в ІТС ОДС ОР;
– організація та здійснення заходів з резервного копіювання та відновлення критичної інформації, що зберігається у ІТС ОДС ОР.

3.4.2.2 Основними функціями користувача з роллю "системний адміністратор" є:

– налаштування, моніторинг працездатності та модернізація КТЗ ІТС ОДС ОР;
– установка, модернізація, налаштування та моніторинг працездатності системного і функціонального (прикладного) ПЗ у ІТС ОДС ОР;
– налаштування, контроль працездатності та модернізація комунікаційного (мережного) обладнання;
– ведення та актуалізація Microsoft Active Directory - бази даних користувачів та комп'ютерів домену;
– супровід, налаштування, актуалізація та моніторинг працездатності корпоративної пошти;
– моніторинг мережі та виявлення слабких місць;
– призначення мережних адрес компонентам ІТС ОДС ОР;
– налаштування правил маршрутизації;
– налаштування та підтримка мережних сервісів;
– налаштування ФПЗ;
– організація та здійснення заходів з резервного копіювання та відновлення у ІТС ОДС ОР, відповідно до інструкції з резервного копіювання та відновлення.

3.4.2.3 Основними функціями користувача з роллю "адміністратор БД" є:

– налаштування СКБД;
– контроль функціонування та оптимізація працездатності СКБД;
– налаштування системи автоматичного резервного копіювання та контроль за її функціонуванням;
– відновлення інформації у БД;
– забезпечення доступності БД;

- розмежування прав доступу до БД згідно з правилами розмежування доступу;
- оновлення таблиць БД;
- локалізація та усунення помилок в роботі СКБД;
- налаштування реплікації БД.

3.4.2.4 Основними функціями користувача з роллю "внутрішній користувач", що є посадовою особою Держстату, призначений для виконання посадових обов'язків в рамках функціонування ІТС ОДС ОР, є:

– створення, редагування та видалення електронних документів;
– приймання та відправлення електронної пошти;
– обробка та аналіз статистичної інформації;
– проведення статистичних досліджень;
– надання виписок з БД ЄДРПОУ в паперовій формі;
– виконання інших задач в ІТС, що передбачені посадовими інструкціями співробітників.
– виконання інших задач в підсистемах, що передбачені посадовими інструкціями співробітника.

3.8 Умови розташування об'єкта

3.8.1 Розміщення обчислювальної системи компонентів ІТС ОДС ОР має виконуватися, виходячи з:

– локалізації технічних засобів у приміщеннях, фізичний доступ до яких є обмеженим;
– технічних характеристик обладнання і вимог щодо його встановлення і умов експлуатації визначених їх виробником.

3.8.2 Приміщення, де розміщуються компоненти ІТС ОДС ОР знаходяться у складі ГУС області.

3.8.3 Приміщення, де розміщуються компоненти ІТС ОДС ОР мають пропускний і внутрішньо об'єктовий режим, що визначені діючими нормативними та розпорядчими документами Держстату.

3.9 Технологія обробки інформації в ІТС

Обробка інформації включає:

- збирання первинних даних;
- ведення обліку звітів респондентів;
- обробку первинних даних;
- аналіз статистичної інформації;
- поширення статистичної інформації;
- ведення єдиного державного реєстру підприємств та організацій України;
- електронний документообіг;
- адміністрування.
- Збирання первинних даних здійснюється шляхом:
- отримання даних з центрального рівня ОДС у форматі .dbf;

– внесення даних зі звітів підприємств і організацій (у т.ч. шляхом оптичного розпізнавання символів).

Збирання первинних даних здійснюється у відділах збирання, обробки, аналізу та поширення статистичної інформації.

Ведення обліку звітів респондентів здійснюється через підсистему "Єдине вікно", що використовується виключно в деяких ГУС. "Єдине вікно" функціонує як БД в .dbf форматі, доступ до якого надається з використанням Access 2003. Можуть бути і інші варіанти виконання даної підсистеми.

Обробка первинних даних та аналіз статистичної інформації здійснюються у ПЗ власної розробки, яке розробляється засобами SQL Anywhere, PASW Statistics, Visual FoxPro, PowerDesigner. ПЗ встановлене на серверах ІТС ОДС обласного рівня. Розробка ПЗ здійснюється співробітниками ГУС. Обробка первинних даних та аналізу статистичної інформації здійснюються у підсистемі збирання, обробки, аналізу та поширення статистичної інформації.

Обробка статистичної інформації здійснюється в ІССІ, ядро якої знаходиться в ІТС ОДС ЦР, та КЕОІ. Обмін даними відбувається за технологією реплікації.

Поширення статистичної інформації здійснюється шляхом публікації звітів та результатів аналізу статистичної інформації на веб-сайті Державної служби статистики України та веб-сайтах Головних управлінь статистики у областях.

Електронний документообіг здійснюється шляхом сканування та завантаження у систему електронного документообігу "Megapolis.DocNet" зображень, отриманих скануванням паперових документів. На стороні ІТС ОДС ОР використовуються веб-браузери для роботи з СЕДО.

Поштові сервіси розміщено у складі ІТС ОДС ЦР. Користувачі ІТС ОДС ОР з використанням поштових клієнтів підключаються до поштових сервісів ІТС ОДС у складі центрального рівня. Обмін поштовими повідомленнями передбачає доступ користувачів до поштового сервера з використанням поштового клієнта. В даних повідомленнях не містяться відомості з конфіденційною інформацією, виключно відкрита інформація. Доступ до повідомлень користувач отримує відповідно до власного логіну та паролю, розмежування доступу виконується механізмами ПК поштового серверу на базі ІТС ОДС ЦР. Доступ для обміну поштовими повідомленнями мають всі користувачів та адміністратори ІТС ОДС ОР.

Для управління обліковими записами користувачів зі складу ІТС ОДС ОР використовується домен. ІТС ОДС ЦР формує єдиний домен для ІТС ОДС на всіх рівнях, включаючи регіональний. Керування обліковими записами здійснюється адміністраторами ІТС ОДС ЦР, а в обласному формується субдомен для керування обліковими записами ІТС ОДС ОР та ІТС ОДС ОР власними адміністраторами. Крім того ІТС ОДС ОР має власні контролери домену для організації роботи користувачів, що знаходяться в ізольованих мережах.

У складі ІТС ОДС ЦР розгорнуто технологічний ЦСК для випуску та обслуговування сертифікатів відкритих ключів користувачів ІТС ОДС. Даний ЦСК використовується для

обслуговування сертифікатів, що призначені для шифраторів, які в свою чергу забезпечують шифрування інформації між ІТС ОДС ОР та ІТС ОДС ЦР (IP-шифраторами).

У складі ІТС ОДС ОР та ІТС ОДС ЦР розгорнуто файлові сервери і користувачі ІТС ОДС використовуються їх для експорту інформації на всі рівні ІТС ОДС, крім того обмін інформацією відбувається і з використанням поштових повідомлень.

РС користувачів ІТС ОДС ОР використовується для:

– роботи з електронними документами;

– роботи з електронною поштою;

– проведення статистичних досліджень і введення первинної статистичної інформації (робота у ІССІ та КЕОІ);

– робіт в БД ЄДРПОУ.

Технологія роботи в ІТС ОДС ОР передбачає використання окремих РС для виконання даних функціональних задач, а також використання однієї РС для виконання всіх поставлених задач. Для передачі даних між РС у ЛОМ ІТС ОДС ОР може використовуватись з'ємний носій чи спільна директорія.

З обласного рівня проконтрольовані первинні звіти передаються засобами телекомунікаційного зв'язку за допомогою корпоративної мережі Держстату або Інтернету (електронна пошта) до центрального рівня.

Схема обробки інформації в КЕОІ на всіх рівнях ІТС ОДС показана на рис.3.3. Детально опис процедури для кожної форми звіту подається окремим документом і затверджується керівником Держстату.

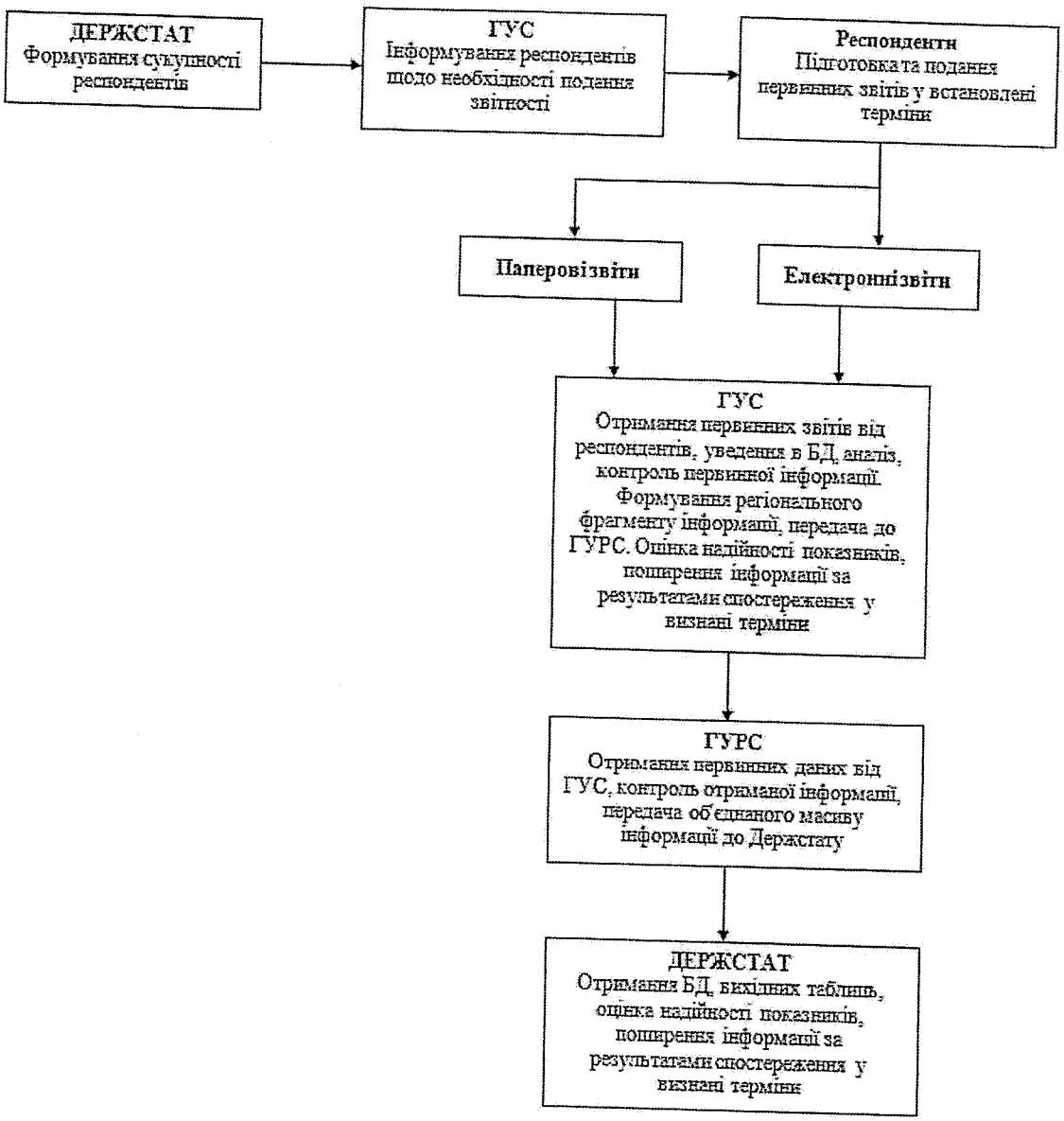


Рисунок 3.3 - Схема організації збору, обробки й проходження даних

Робота у ІССІ передбачає використання клієнта доступу для проведення/виконання державного статистичного спостереження. Реєстр користувачів системи містить сформований на визначену дату перелік активних користувачів усіх вузлів ІССІ.

У процесі проведення робіт з уведення й обробки статистичної інформації фахівці Держстату, які беруть участь у проведенні/виконанні ДСС, повинні керуватися відповідною експлуатаційною документацією на Систему, зокрема:

– керівництво користувача АРМ "Статистик";
– керівництво користувача АРМ "Аналітик";
– керівництво користувача АРМ "Адміністратор".

Процес адміністрування та супроводження ІССІ забезпечується ІТ-фахівцями Держстату та ГУС і полягає у керуванні, технічному обслуговуванні та проведенні інших технічних й адміністративних заходів, спрямованих на підтримку ІССІ у робочому стані.

АРМ "Статистик" – розгортається на регіональному рівні, забезпечує процеси: введення первинних даних від респондентів за формами звітності, перегляд протоколів, виконання контролю, виправлення помилок за результатами контролю, введення та обробки даних статистичних спостережень. .

На обласному рівні звіти на паперових носіях, отримані від респондентів, вводяться до БД КЕОІ та/або надаються на центральний рівень. Під час введення в БД або отримання звітів у паперових носіях, проводиться первинний контроль звітів.

Ведення Єдиного державного реєстру підприємств та організацій України здійснюється шляхом виділення номерів (кодів ЄДРПОУ) при реєстрації підприємств та організацій з наперед призначеного інтервалу номерів. Дані номери централізовано надходять до ІТС ОДС ЦР і потім засобами електронної пошти раз на добу передаються (актуальна база на момент часу) до ІТС ОДС ОР, які в свою чергу надають дану базу до ІТС ОДС ОР. У випадку звернення громадян, користувач ІТС ОДС ОР з РС на якій встановлено СКБД для ЄДРПОУ надає довідку, шляхом її друку на принтері.

3.10 Можливі загрози безпеки інформації

Порушення конфіденційності, цілісності та доступності інформації, що обробляється у ІТС ОДС ОР можуть проявлятися внаслідок таких загроз:

– загрози порушення конфіденційності, цілісності (в тому числі, достовірності та автентичності) та доступності конфіденційної інформації;

– загрози порушення цілісності та доступності відкритої інформації;

– загрози порушення доступності, конфіденційності та цілісності технологічної інформації.

Порушення конфіденційності, цілісності та доступності інформації, що обробляється у ІТС ОДС ОР можуть проявлятися внаслідок реалізації таких загроз:

– підробка (навмисне порушення достовірності) інформації користувачами ІТС ОДС ОР;

– порушення правил розмежування доступу до інформації, що обробляється в компонентах ІТС ОДС ОР внаслідок неправильної конфігурації та/або обходу механізмів КЗЗ;

– порушення властивостей конфіденційності, цілісності або доступності інформації внаслідок некомпетентності або недбалості користувачів;

– втрата атрибутів доступу користувачів ІТС ОДС ОР, що призводить до неможливості використання його функцій;

– втрата керованості над ІТС ОДС ОР внаслідок пошкодження даних або окремих програмних чи програмно-апаратних засобів;

– несанкціоноване отримання або викривлення даних початкової ідентифікації та автентифікації користувача;

– здійснення порушником доступу на запис/видалення до інформаційних об'єктів ІТС ОДС ОР від імені уповноваженого користувача;

– несанкціоноване перехоплення/викривлення порушником даних, що передаються каналами зв'язку;

– здійснення порушником доступу на читання до інформаційних об'єктів ІТС ОДС ОР від імені уповноваженого користувача;

– здійснення користувачем дій, що порушують політику безпеки внаслідок надання йому повноважень, що не потрібні йому для виконання посадових обов'язків;

– неправильне функціонування складових ІТС ОДС ОР внаслідок порушення цілісності програмних або апаратно-програмних засобів чи інших відмов;

– несанкціоновані дії порушника шляхом зламу (НСД до) КЗЗ або внаслідок збоїв у роботі КЗЗ;

– модифікація або видалення даних з журналів реєстрації подій порушником.

4 ВИМОГИ ТА ФУНКЦІЇ КЗЗ ІТС

4.1 Загальні вимоги до КЗЗ ІТС

Враховуючи реалізовані у ІТС ОДС ОР технології обробки інформації, для КЗЗ ІТС ОДС ОР висуваються такі загальні вимоги (цілі безпеки), КЗЗ ІТС ОДС ЦР має:

– гарантувати, що атрибути доступу (користувачів та пасивних об'єктів) на основі яких реалізується політика розмежування доступу може змінювати лише вповноважений на це користувач;

– забезпечити реєстрацію подій, що мають відношення до безпеки;

– має забезпечити захист від несанкціонованого отримання (перехоплення) або викривлення даних ідентифікації та автентифікації користувачів;

– забезпечити можливість здійснити відновлення компонентів, що були виведенні з ладу у наслідок реалізації атаки чи випадкового збою;

– забезпечувати доступ на читання, модифікацію та видалення інформації, яка обробляється в ІТС ОДС ОР тільки для авторизованих користувачів відповідно до їх прав доступу;

– забезпечувати розмежування доступу користувачів до функцій та інформаційних ресурсів відповідно до їх прав доступу;

– забезпечити захист від несанкціонованого ознайомлення та модифікації інформації, що передається каналами зв'язку;

– забезпечувати автентифікацію КЗЗ, що взаємодіють через канали зв'язку;

– здійснювати реєстрацію подій, які мають відношення до безпеки інформації захищати журнали реєстрації подій, що ведуться його компонентами;

– гарантувати, що неправильні дії користувача з використання ресурсів ІТС, не призведуть до недоступності цього виду ресурсів для інших користувачів;

– реалізовувати політику мінімізації повноважень користувачів ІТС ОДС ОР;

– забезпечувати захищений обмін для конфіденційної інформації з іншими ІТС;

– забезпечувати захист власних компонентів та інформаційних ресурсів від мережних атак;

– надавати можливість контролю за своєю роботою зі сторони осіб, які відповідають за забезпечення безпеки інформації у ІТС ОДС ОР.

4.2 Вимоги до складу КЗЗ ІТС ОДС ОР

Враховуючи результати аналізу загроз та цілі безпеки висуваються такі вимоги до складу програмних та апаратно-програмних компонентів КЗЗ у складі ІТС ОДС ОР:

– КЗЗ ОС серверів з лінійки Windows;
– КЗЗ ОС серверів з лінійки Unix;
– КЗЗ ОС РС;
– КЗЗ ФПЗ ІССІ;
– КЗЗ СКБД;
– ПЗ антивірусного захисту;
– ПК віддаленого управління IP-шифратора

– IP-шифратор;
– МЕ;
– АПЗ КЗІ.

4.3 Функції та вимоги до складових (компонентів) КЗЗ ІТС ОДС ОР

4.3.1 Функції та вимоги до КЗЗ ОС серверів з лінійки Windows

КЗЗ ОС серверів з лінійки Windows повинен реалізовувати такі функції:

– забезпечення власної цілісності та об'єктів-процесів, що функціонують під її керуванням;
– ідентифікація та автентифікація користувачів на основі логіна та пароля;
– ідентифікація та автентифікація користувачів домену на основі логіна та пароля;
– централізоване керування обліковими записами ОС для РС в межах домену ІТС ОДС ЦР;
– керування обліковими записами користувачів;
– розмежування доступу на читання, модифікацію та запуск до системних файлів та утиліт, а також на доступ до журналів ОС;
– надання достовірного каналу для введення атрибутів користувачів ОС;
– забезпечення безперервності функціонування ОС;
– автоматичне відновлення ОС після збоїв;
– відновлення стану ОС на певний момент часу;
– ведення журналів реєстрації подій.

4.3.2 Функції та вимоги до ОС серверів з лінійки Unix

КЗЗ ОС серверів з лінійки Unix повинен реалізовувати такі функції:

– забезпечення власної цілісності та об'єктів-процесів, що функціонують під її керуванням;
– ідентифікація та автентифікація користувачів на основі логіна та пароля;
– керування обліковими записами користувачів;
– розмежування доступу на читання, модифікацію та запуск до системних файлів та утиліт, а також на доступ до журналів ОС;
– надання достовірного каналу для введення атрибутів користувачів ОС;
– забезпечення безперервності функціонування ОС;
– автоматичне відновлення ОС після збоїв;
– відновлення стану ОС на певний момент часу;
– ведення журналів реєстрації подій.

4.3.3 Функції та вимоги до КЗЗ ОС для РС

КЗЗ ОС для РС повинен реалізовувати такі функції:

– забезпечення власної цілісності та об'єктів-процесів, що функціонують під її керуванням;

– ідентифікація та автентифікація користувачів на основі логіна та пароля;

– керування обліковими записами користувачів;

– розмежування доступу на читання, модифікацію та запуск до системних файлів та утиліт, а також на доступ до журналів ОС;

– надання достовірного каналу для введення атрибутів користувачів ОС;

– забезпечення безперервності функціонування ОС;

– ведення журналів реєстрації подій.

4.3.4 Функції та вимоги до КЗЗ ФПЗ ІССІ

КЗЗ ФПЗ ІССІ має реалізовувати такі функції:

– ідентифікація та автентифікація користувачів;
– розмежування прав доступу до об'єктів захисту;
– керування обліковими записами користувачів;
– управління журналами реєстрації подій, моніторинг дій користувачів;
– керування атрибутами користувачів;
– відкат (може бути покладено на СКБД).

4.3.5 Функції та вимоги до КЗЗ СКБД

КЗЗ СКБД повинен реалізовувати такі функції:

– відкат БД у випадку помилок;

– розмежування доступу на читання та модифікацію об'єктів (таблиць, відображень, процедур, що зберігаються) БД;

– ідентифікація та автентифікація користувачів СКБД на основі логіна та пароля;

– реєстрація подій, що відбуваються на рівні СКБД;

– підтримка множини локальних адміністративних та користувальницьких ролей на рівні СКБД;

– підтримка механізму реплікацій;

– можливість роботи в кластері.

4.3.6 Функції та вимоги до МЕ

МЕ повинен реалізовувати такі функції:

– розмежування мережних потоків за правилами встановленими відповідним користувачем;

– контроль та інспекція мережних протоколів;

– розмежування доступу на читання та модифікацію налаштувань;

– ідентифікація та автентифікація користувачів за логіном та паролем;

– відновлення налаштувань МЕ на певний момент часу з використанням резервних копій;

– контроль цілісності вбудованого програмного забезпечення;

– ведення та зберігання записів про мережеві підключення.

4.3.7 Функції та вимоги до ПЗ антивірусного захисту інформації

ПЗ антивірусного захисту інформації повинен реалізовувати такі функції:

– контроль власної цілісності;

– захист від зловмисного ПЗ та вірусних заражень;

– автоматичне тестування на предмет вірусного зараження при старті ОС, будь-якого додатку та за запитом уповноваженого користувача;

– автоматичне тестування на предмет вірусного зараження при доступі (читанні, копіюванні) файлів з виконуваними розширеннями;

– аудит виявлених порушень.

4.3.8 Функції та вимоги до IP-шифратора

В якості IP-шифратора повинен застосовуватися апаратний засіб. IP-шифратор повинен мати чинний експертний висновок Адміністрації Держспецзв'язку України в сфері КЗІ та реалізовувати такі функції:

- шифрування та контроль цілісності IP-пакетів;
- інкапсуляцію IP-пакетів та їх маршрутизацію між мережевими інтерфейсами;
- прийом та введення в дію ключових даних;
- встановлення захищених з'єднань з іншими IP-шифраторами зі складу ІТС ОДС;
- контроль власної цілісності і правильності функціонування.

4.3.9 Функції та вимоги до АПЗ КЗІ

У якості АПЗ КЗІ повинні використовуватися апаратно-програмні засоби, що мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації та має реалізовувати такі функції:

– ідентифікація та автентифікація користувачів АПЗ КЗІ за паролем;

– забезпечення конфіденційності та контролю цілісності даних, які передаються між АПЗ КЗІ та автентифікованими програмними засобами користувача (ЕОМ);

– контроль цілісності вбудованого програмного забезпечення;

– тестування правильності криптографічних перетворень.

4.3.10 Функції та вимоги до ПК віддаленого управління IP-шифратора

ПК віддаленого управління IP-шифратора повинно реалізовувати такі функції:

- автентифікація засобу захисту при мережній взаємодії;
- забезпечення конфіденційності та контролю цілісності даних, що передаються між IP-шифратором та ПК управління;
- забезпечення достовірного каналу для введення атрибутів доступу до особистого ключа;
- реалізація клієнтської частини протоколу ідентифікації та автентифікації користувача IP-шифратора та ПК управління (з метою адміністрування);
- тестування правильності криптографічних перетворень.

4.4 Вимоги до функцій криптографічного захисту інформації

У якості засобів, які реалізують функції криптографічного захисту інформації (у тому числі засоби формування та перевірки ЕП) повинні використовуватися засоби, які мають чинний, позитивний експертний висновок Адміністрації Держспецзв'язку в сфері КЗІ.

4.5 Вимоги до функцій мережевого захисту інформації

У якості засобів, які реалізують функції мережевого захисту інформації в ІТС ОДС ОР (міжмережеві екрани) повинні використовуватися засоби, які мають позитивний експертний висновок Адміністрації Держспецзв'язку в сфері ТЗІ. За можливості повинні використовуватись апаратні засоби.

4.6 Вимоги до функцій антивірусного захисту інформації

У якості засобів, які реалізують функції антивірусного захисту інформації повинні використовуватися засоби, які мають чинний, позитивний експертний висновок Адміністрації Держспецзв'язку в сфері ТЗІ.

Оновлення ПЗ антивірусного захисту має здійснюватися відповідно до "Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації", затвердженого наказом Адміністрації державної служби спеціального зв'язку та захисту інформації України № 45 від 26.03.2007 р.

4.7 Інші вимоги

Доступ ІТС ОДС ОР до мережі Інтернет повинен здійснюватися через захищений вузол інтернет-доступу.

Підключення інших ІТС до ІТС ОДС ОР можливе лише за наявності у них атестата відповідності на комплексну систему захисту інформації.

5 ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

5.1 Вимоги до КСЗІ в ІТС в частині захисту від несанкціонованого доступу

5.1.1 Об'єкти захисту

У процесі функціонування ІТС ОДС ОР об'єктами захисту є: програмно-інформаційні ресурси, в яких знаходиться, або може знаходитись інформація, яка підлягає захисту, а також програмне забезпечення, що реалізує технології оброблення такої інформації, для виконання персоналом ІТС ОДС ОР своїх функцій.

Відповідно до функціонального призначення, місця розміщення та виду представлення, політикою безпеки визначається наступний узагальнений перелік інформаційних ресурсів (таблиця 5.1).

Атрибутами доступу об'єктів доступу у вигляді файлів є назва файлу, а об'єктів БД – назва таблиці БД.

Таблиця 5.1 – Перелік та позначення інформаційних ресурсів ІТС ОДС ОР

№	Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС ОДС ЦР
1.	{Д_ТІ}	Технологічна інформація ІТС ОДС ОР	Конфіденційна інформація	Об'єкти файлової системи (далі – ФС), Об'єкти БД
2.	{Д_ЖУР}	Журнали реєстрації системних подій ІТС ОДС ОР	Конфіденційна інформація	Об'єкти ФС, Об'єкти БД, Об'єкти веб-сторінки
3.	{Д_ПСД}	Первинні статистичні дані (звіти підприємств та організацій)	Конфіденційна інформація	Об'єкти БД, Об'єкти ФС
4.	{Д_СІ}	Статистична інформація (результати обробки первинних статистичних даних, статистичні завдання тощо)	Відкрита інформація	Об'єкти БД, Об'єкти ФС
5.	{Д_ЕД}	Документи у СЕДО, резолюції	Відкрита інформація	Об'єкти БД, Об'єкти ФС, Об'єкти веб-сторінки
6.	{Д_Ф}	Файли на файлових серверах	Відкрита інформація	Об'єкти ФС
7.	{Д_ЄДРПОУ}	Дані ЄДРПОУ	Відкрита інформація	Об'єкти БД, Об'єкти ФС
8.	{Д_ДОВ}	Довідники і класифікатори	Відкрита інформація	Об'єкти БД, Об'єкти ФС, Об'єкти веб-сторінки
9.	{Д_ПШТ}	Поштові повідомлення	Відкрита інформація	Об'єкти ФС
10.	{Д_СЕР}	Сертифікати ЦСК Держстату та КНЕДП, шифраторів, зареєстрованих користувачів, адміністраторів, списки відкликаних	Відкрита інформація[1]	Об'єкти ФС

[1] Сертифікати користувачів можуть відноситися до ІзОД (ПД за вимогою користувачів)

№	Позначення	Назва	Ступінь обмеження доступу	Представлення в ІТС ОДС ЦР
		сертифікатів		
11.	{Д_ОКК}	Особисті ключі користувачів чи засобів КЗІ	Конфіденційна інформація	Об'єкти ФС, об'єкти АПЗ КЗІ

5.1.2 Користувачі та процеси

За рівнем повноважень щодо доступу до програмних засобів, інформації, що циркулює та накопичується у ІТС ОДС ОР, характером та змістом робіт, які виконуються в процесі функціонування, користувачі можуть мати одну або кілька з наведених нижче ролей:

– "адміністратор безпеки" (К_АБ);
– "системний адміністратор" (К_АС);
– "адміністратор БД" (К_АБД);
– "внутрішній користувач" (К_ВК).

КЗЗ ІТС ОДС ОР повинен реалізовувати розмежування доступу до об'єктів захисту (п. 5.1.1) з боку об'єктів-користувачів(п. 5.1.2)на основі атрибутів доступу об'єктів захисту та об'єктів-користувачів. Об'єкт-користувач є поданням фізичного користувача у ІТС ОДС ОР, що створюється в процесі входження (здійснення процедури ідентифікації та автентифікації) користувача у ІТС ОДС ОР і повністю характеризується унікальним набором атрибутів (наприклад, власним ідентифікатором та ідентифікатором локальної ролі).

Атрибути доступу користувачів та процесів використовуються для ідентифікації та автентифікації. Атрибути доступу об'єкта користувача та об'єкта процесу використовуються для розмежування доступу до об'єктів захисту ІТС ОДС ОР.

Атрибути доступу об'єктів захисту використовуються КЗЗ для розмежування доступу до них.

Атрибути доступу категорій користувачів та об'єктів-користувачів, що мають відповідні ролі наведені у таблиці 5.2.

Таблиця 5.2 – Опис атрибутів доступу, що мають користувачі ІТС ОДС ОР згідно наданих їм ролей

Суб'єкт доступу / Назва атрибуту	К_АБ	К_АС	К_АБД	К_ВК
Ідентифікатори та паролі до облікових записів ОС серверів (адміністративні)	+	+		
Ідентифікатори та паролі до облікових записів ОС серверів (користувацькі)			+	
Ідентифікатори та паролі до облікових записів ОС РС в домені (адміністративні)	+	+		
Ідентифікатори та паролі до облікових записів ОС РС в домені (користувацькі)			+	+

Назва атрибуту \ Суб'єкт доступу	К_АБ	К_АС	К_АБД	К_ВК
Логін та пароль до облікових записів СЕДО	+/-	+/-	+/-	+/-
Логін та пароль до облікових записів ФПЗ (адміністративний)	+	+		
Логін та пароль до облікових записів ФПЗ (користувацький)			+	+
Логін та пароль до облікових записів СКБД	+		+	
Логін та пароль до поштових сервісів	+	+	+	+
Ідентифікатори локальних ролей та паролі до облікових записів МЕ	+	+		
Ідентифікатори локальних ролей та паролі до комунікаційного та іншого обладнання		+		
Паролі до облікових записів ПЗ АЗ	+	+		
Особистий ключ КЕП, відповідний сертифікат відкритого ключа та пароль доступу до ключа[2]	-	-	-	+/-
Особистий ключ IP-шифратора, ПК віддаленого керування відповідний сертифікат відкритого ключа та пароль доступу до ключа	+			

5.1.3 Правила розмежування доступу

Усі запити користувачів на доступ до об'єкту захисту повинні оброблятися КЗЗ. Доступ до пасивного об'єкту захисту має дозволятися/заборонятися згідно правил розмежування доступу за результатами порівняння атрибутів доступу об'єкта-користувача, об'єкта-процесу та призначених йому прав. Права доступу, що їх має контролювати КЗЗ ІТС ОДС ОР, об'єктів-користувачів та об'єктів-процесів до інформаційних ресурсів визначені у таблиці 5.3.

При розмежуванні доступу використовується адміністративне керування доступом до об'єктів захисту, а до {Д_Ф} – кожен користувач також може встановлювати власні права доступу.

Право на налаштування та інсталяцію/деінсталяцію компонентів надано тільки користувачам з ролями К_АБ або К_АС в ІТС ОДС ОР. При цьому К_АС відповідно мають дозвіл на модифікацію налаштувань, що не стосуються безпеки.

Права користувачів на використання ПЗ ІТС ОДС ОР визначаються наявністю атрибутів доступу, що зведені до таблиці 5.2.

[2]Особистий ключ повинен бути, якщо внутрішні користувачі ІТС здійснює доступ до СЕДО

Таблиця 5.3 – Максимальні права доступу до інформаційних ресурсів, що мають процеси та користувачі ІТС ОДС ОР згідно наданих їм ролей

Об'єкт захисту	Право доступу			
	Читання	Модифікація	Створення	Видалення[3]
{Д_ТІ}[4]	К_АБ, К_АС, К_АБД	К_АБ, К_АС[5], К_АБД	К_АБ, К_АС[5], К_АБД	-
{Д_ЖУР}[4]	К_АБ, К_АС, К_АБД	-	-	К_АБ
{Д_ПСД}	К_АБД, К_ВК	-	К_ВК	-
{Д_СІ}	К_АБД, К_ВК	К_ВК	К_ВК	К_ВК
{Д_ЕД}	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК
{Д_Ф}	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК
{Д_ПШТ}	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК	К_АБД, К_АБ, К_АС, К_ВК
{Д_ЄДРПОУ}	К_ВК	-	-	-
{Д_ДОВ}	К_АС, К_ВК	К_ВК	К_ВК	К_ВК
{Д_СЕР}	ВСІ	-	К_АБ[6]	К_АБ
{Д_ОКК}[7]	К_АБ, К_ВК	-	К_АБ, К_ВК	К_АБ, К_ВК

5.1.4 Вимоги до організаційних заходів

5.1.4.1 Забезпечення безпеки об'єктів захисту у ІТС ОДС ОР має здійснюватися шляхом комплексного використання організаційних (адміністративних) заходів, правових і законодавчих норм, фізичних і технічних (програмних, апаратно-програмних і апаратних) засобів захисту інформації.

5.1.4.2 Основні організаційні заходи повинні передбачати:

– створення відповідального підрозділу, якому надаються повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації – служби захисту інформації у ІТС ОДС ОР (далі – СЗІ ІТС ОДС ОР);

– організацію проведення обстеження середовища функціонування ІТС ОДС ОР;

– визначення політики безпеки інформації у ІТС ОДС ОР;

– розробку й впровадження плану захисту інформації у ІТС ОДС ОР;

– реалізацію положень політики безпеки;

– порядок реєстрації у ІТС ОДС ОР всіх користувачів і їх дій з об'єктами захисту;

– регламентацію доступу користувачів різних категорій до об'єктів захисту ІТС ОДС ОР;

– порядок проведення модернізації КСЗІ в ІТС ОДС ОР та її окремих складових;

– порядок зв'язку з іншими ІТС.

---

[3]Під правом "видалення" для {Д_ЖУР} мається на увазі їх повне очищення

[4]К_АБД має вказаний доступ лише в СКБД

[5]К_АС має вказаний доступ лише з дозволу К_АБ

[6]У тому випадку, якщо {Д_СЕР} обслуговується внутрішнім (технологічним) ЦСК Держстату

[7]К_АБ має доступ також і до особистих ключів шифратора

5.1.4.3 Фізична цілісність критичних апаратних компонентів повинна забезпечуватися організаційними заходами й застосуванням пломб (наліпок, печаток та ін.) на блоках і пристроях засобів обчислювальної техніки. Повсякденний контроль цілісності й відповідності печатки (пломб, наліпок) на системному блоці РС повинен здійснюватися користувачами. Періодичний контроль – адміністратором.

5.1.4.4 На правовому рівні для забезпечення безпеки інформації повинні бути розроблені рішення, відносно:

– системи нормативно-правового забезпечення робіт із захисту інформації у ІТС ОДС ОР;

– процедур доведення до персоналу ІТС ОДС ОР основних положень політики безпеки інформації, їхнього навчання й підвищення кваліфікації з питань безпеки інформації;

– системи контролю своєчасності, ефективності й повноти реалізації у ІТС ОДС ОР рішень із захисту інформації, дотримання персоналом положень політики безпеки.

На технічному рівні для блокування загроз НСД до інформаційних ресурсів ІТС ОДС ОР необхідне застосування КЗЗ (вимоги, що висуваються та функції складових КЗЗ ІТС ОДС ОР наведені у п. 4) у складі обчислювальної системи ІТС ОДС ОР.

5.1.4.5 У основу політики безпеки КЗЗ ІТС ОДС ОР повинен бути покладений адміністративний принцип розмежування доступу до об'єктів захисту.

5.1.4.6 У обчислювальній системі ІТС ОДС ОР адміністратор безпеки є спеціально авторизованим користувачем (роль "розпорядника (власника)"), якому надані повноваження щодо керування потоками інформації від захищених об'єктів (файлів даних системи захисту, файлів ведення захищеного журналу реєстрації подій, функціональних програм оброблення інформації та КЗЗ, процесів тощо) до користувачів.

5.1.4.7 Адміністративний принцип розмежування доступу до об'єктів захисту, що зберігаються на машинних носіях великої ємності, повинен забезпечуватися впровадженням таких організаційних заходів:

– співробітник СЗІ здійснює контроль доступу користувачів до об'єктів захисту;

– фізичний доступ у приміщення де розміщуються компоненти ІТС ОДС ОР здійснюється згідно списку та контролюється співробітниками охорони;

– склад обчислювальної системи ІТС ОДС ОР визначено формуляром і його незмінність контролюється адміністратором безпеки;

– у складі програмного забезпечення ІТС ОДС ОР відсутні програми, які не призначені для вирішення дозволених функціональних завдань;

– користувачам заборонено встановлювати будь-яке програмне забезпечення на компоненти ІТС ОДС ОР.

5.1.4.8 На адміністратора безпеки покладається виконання таких функцій:

– адміністрування облікових записів користувачів;

– моніторинг подій ОС, СКБД, апаратного забезпечення, СПЗ, МЕ та іншого програмного та апаратного забезпечення;

– адміністрування засобів антивірусного захисту;

– адміністрування засобів КЗІ.

5.1.4.9 В ІТС ОДС ОР користувач, який намагається одержати доступ до ресурсів, повинен виконати в обов'язковому порядку процедуру входу (реєстрації) у систему. При вході в систему повинна здійснюватися ідентифікація (розпізнавання) і автентифікація (підтвердження автентичності) користувача (суб'єкта) з використанням атрибутів, що визначені у п. 5.1.2.

5.1.4.10 Технічний персонал ІТС ОДС ОР, постачальники устаткування й фахівці, що здійснюють монтаж і обслуговування технічних засобів ІТС ОДС ОР і не мають дозволу на доступ до даних, можуть мати доступ до програмних і апаратних засобів ІТС ОДС ОР лише під час робіт з тестування й інсталяції програмного забезпечення, установки й регламентного обслуговування устаткування та ін. Зазначені категорії осіб повинні мати дозвіл на доступ тільки до відомостей, які утримуються в програмній і технічній документації на обчислювальну систему ІТС ОДС ЦР або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

5.1.5 Семантика профілів прийнята відповідно до НД ТЗІ 2.5-004-99.

5.1.6 Послуги безпеки, що реалізуються у КЗЗ складових частин ІТС ОДС ОР, повинні бути реалізовані з рівнем гарантій Г-2. Специфікації всіх критеріїв гарантій повинні в повному обсязі відповідати НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

5.1.7 КЗЗ ІТС ОДС ОР має реалізовувати такий профіль захищеності:

{КА-2, КВ-1, ЦА-1, ЦД-1, ЦО-1, ЦВ-1, ДС-1, ДВ-1, ДЗ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-2}.

5.2 Специфікації вимог для КЗЗ ІТС ОДС ОР

5.2.1 Базова адміністративна конфіденційність (КА-2)

5.2.1.1 КЗЗ ІТС ОДС ОР має надавати адміністраторам можливість керувати потоками інформації від пасивних об'єктів захисту до об'єктів-користувачів з метою захисту пасивних об'єктів захисту від несанкціонованого ознайомлення з їх вмістом (компрометації).

5.2.1.2 Політика послуги має відноситися до множини пасивних об'єктів захисту: {Д_ТІ}, {Д_ЖУР}, {Д_ПСД}, {Д_ОКК} та користувачів ІТС ОДС ОР всіх категорій.

5.2.1.3 КЗЗ ІТС ОДС ОР повинен здійснювати розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

5.2.1.4 КЗЗ ІТС ОДС ОР має аналізувати усі запити на доступ від імені об'єктів-користувачів, що надаються з метою одержання інформації, яка міститься в пасивних об'єктах захисту. КЗЗ ІТС ОДС ОР має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.3), а також значень, що містяться у списках керування доступом.

5.2.1.5 Запити на зміну прав доступу до наступних підмножин пасивних об'єктів захисту:

– {Д_ТІ}, {Д_ЖУР} (крім СКБД) повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБ та/або К_АС;

– {Д_ТІ}, {Д_ЖУР} (у частині СКБД)повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБД;

– {Д_ПСД} повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБ;

– {Д_ОКК} не повинні оброблятися КЗЗ ІТС ОДС ОР.

5.2.1.6 КЗЗ ІТС ОДС ОР повинен надавати можливість користувачу з роллю К_АБ визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на одержання інформації, що міститься в пасивних об'єктах захисту.

5.2.1.7 Права доступу до кожного об'єкта захисту повинні встановлюватися в момент його створення.

5.2.1.8 Можливість керування правами на ініціювання, виконання процесів у процесі функціонування ІТС ОДС ОР не передбачається.

5.2.1.9 При експорті (резервному копіюванні) об'єктів {Д_ОКК} повинен зберігатися атрибут доступу – пароль. Вимог щодо збереження атрибутів доступу до інших пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

5.2.2 Мінімальна конфіденційність при обміні (КВ-1)

5.2.2.1 Послуга "Конфіденційність при обміні" дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

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

5.2.2.3 Політика конфіденційності при обміні, що реалізується КЗЗ ІТС ОДС ОР, повинна відноситись до (реалізовуватися для) {Д_ТІ}, {Д_ПСД} під час їх передачі між компонентами ІТС ОДС ОР та територіальними підрозділами ІТС ОДС.

5.2.2.4 При реалізації політики послуги КЗЗ ІТС ОДС ОР має використовувати {Д_ОКК}, {Д_СЕР}.

5.2.2.5 Політика конфіденційності при обміні, що реалізується КЗЗ ІТС ОДС ОР, повинна реалізовуватись за рахунок використання функцій шифрування. Засоби КЗІ, які використовуються для реалізації функцій шифрування, повинні мати чинний експертний висновок в сфері КЗІ. Користувачі не повинні мати можливості впливати на рівень захисту.

5.2.3 Мінімальна адміністративна цілісність (ЦА-1)

5.2.3.1 Послуга "Адміністративна цілісність" рівня ЦА-1 забезпечує можливість керування потоками інформації від об'єктів-користувачів до захищених пасивних об'єктів з метою захисту пасивних об'єктів від несанкціонованого створення, модифікації або видалення.

5.2.3.2 Політика послуги має відноситися до множини пасивних об'єктів захисту: {Д_ТІ}, {Д_ЖУР}, {Д_ПСД}, {Д_ОКК}, {Д_СІ}, {Д_ЕД} (під час їх обробці в СЕДО), {Д_ПШТ},{Д_ЄДРПОУ}, {Д_ДОВ}, {Д_СЕР} та користувачів ІТС ОДС ОР всіх категорій.

5.2.3.3 КЗЗ ІТС ОДС ОР повинен здійснювати розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

5.2.3.4 КЗЗ ІТС ОДС ОР має аналізувати усі запити на доступ від імені об'єктів-користувачів, що надаються з метою створення/модифікації/видалення інформації, яка

міститься в пасивних об'єктах захисту. КЗЗ ІТС ОДС ОР має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.3), а також значень, що містяться у списках керування доступом.

5.2.3.5 Запити на зміну прав доступу до наступних підмножин пасивних об'єктів захисту:

– {Д_ТІ}, {Д_ЖУР} (крім СКБД), {Д_СІ}, {Д_ЕД} (під час їх обробці в СЕДО), {Д_ДОВ}, {Д_СЕР}, {Д_ЄДРПОУ} повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБ та/або К_АС;

– {Д_ТІ}, {Д_ЖУР} (у частині СКБД) повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБД;

– {Д_ПСД}, повинні оброблятися КЗЗ ІТС ОДС ОР тільки у тому випадку, якщо вони надходять від користувачів з роллю К_АБ;

– {Д_ОКК}, {Д_ПШТ} не повинні оброблятися КЗЗ ІТС ОДС ОР.

5.2.3.6 КЗЗ ІТС ОДС ОР повинен надавати можливість користувачу з роллю К_АБ, К_АС визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на створення/модифікації/видалення інформації, що міститься в пасивних об'єктах захисту.

5.2.3.7 Права доступу до кожного об'єкта захисту повинні встановлюватися в момент його створення.

5.2.3.8 При експорті (резервному копіюванні) об'єктів {Д_ОКК} повинен зберігатися атрибут доступу – пароль. Вимог щодо збереження атрибутів доступу до інших пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

5.2.4 Базова довірча цілісність (ЦД-1)

5.2.4.1 КЗЗ ІТС ОДС ОР має надавати користувачам можливість керувати потоками інформації від пасивних об'єктів захисту до об'єктів користувачів з метою захисту пасивних об'єктів захисту від несанкціонованої модифікації.

5.2.4.2 Політика послуги має відноситися до множини пасивних об'єктів захисту: {Д_ЕД}, {Д_ПШТ} (при збереженні на файлову систему РС зі складу ІТС ОДС ОР), {Д_Ф} та користувачів ІТС ОДС ОР всіх категорій.

5.2.4.3 КЗЗ ІТС ОДС ОР повинен здійснювати розмежування доступу на підставі атрибутів доступу об'єктів користувачів і пасивних об'єктів захисту.

5.2.4.4 КЗЗ ІТС ОДС ОР має аналізувати усі запити на доступ від імені об'єктів користувачів, що надаються з метою модифікації інформації, яка міститься в пасивних об'єктах захисту. КЗЗ ІТС ОДС ОР має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.3), а також значень, що містяться у списках керування доступом.

5.2.4.5 Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ ІТС ОДС ОР на підставі атрибутів доступу користувача, що ініціює запит, і пасивного об'єкта захисту.

5.2.4.6 КЗЗ ІТС ОДС ОР повинен надавати користувачу можливість для кожного захищеного об'єкта {Д_ЕД}, {Д_ПШТ}, {Д_Ф},що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт захисту.

5.2.4.7 Можливість керування правами на ініціювання, виконання процесів у процесі функціонування ІТС ОДС ОР не передбачається.

5.2.4.8 Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

5.2.4.9 Вимоги до експорту та імпорту об'єктів захисту відсутні.

5.2.5 Обмежений відкат (ЦО-1)

5.2.5.1 Послуга "Відкат" рівня ЦО-1 забезпечує можливість скасування операції або послідовності операцій, виконаних над захищеним пасивним об'єктом, з поверненням захищеного об'єкта в попередній стан.

5.2.5.2 Політика послуги має відноситися до множини пасивних об'єктів захисту: {Д_ПСД}, {Д_СІ}, {Д_ДОВ} та користувачів ІТС ОДС ОР К_АБ, К_АБД.

5.2.5.3 КЗЗ ІТС ОДС ОР має надавати автоматизовані засоби, які дозволять користувачам з ролями К_АБ, К_АБД відмінити певний набір (множину) операцій, виконаних над {Д_ПСД}, {Д_СІ}, {Д_ДОВ} за певний проміжок часу.

5.2.5.4 Перелік об'єктів захисту до яких відноситься послуга може уточнюватися на етапі технічного проектування.

5.2.5.5 Факт використання користувачем послуги має реєструватись в системному журналі.

5.2.6 Мінімальна цілісність при обміні (ЦВ-1)

5.2.6.1 Послуга "Мінімальна цілісність при обміні" дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

5.2.6.2 КЗЗ ІТС ОДС ОР повинен забезпечувати захист від модифікації (контроль цілісності) інформації, що міститься в об'єкті, який передається..

5.2.6.3 Політика цілісності при обміні, що реалізується КЗЗ ІТС ОДС ОР, повинна відноситись до (реалізовуватися для) наступних підмножин пасивних об'єктів захисту:

– {Д_ТІ}, {Д_ПСД}, {Д_СІ}, {Д_ЄДРПОУ}під час їх передачі між компонентами ІТС ОДС ОР та територіальними підрозділами ІТС ОДС;

– {Д_ЕД} під час їх передачі між компонентами ІТС ОДС ОР та іншими ІТС.

5.2.6.4 При реалізації політики послуги КЗЗ ІТС ОДС ОР має використовувати {Д_ОКК}, {Д_СЕР}.

5.2.6.5 Політика цілісності при обміні, що реалізується КЗЗ ІТС ОДС ОР, повинна реалізовуватись за рахунок використання функцій КЕП чи шифрування (у режимі виготовлення імітовставки). Засоби КЗІ, які використовуються для реалізації функцій КЗІ, повинні мати чинний експертний висновок в сфері КЗІ. Користувачі не повинні мати можливості впливати на рівень захисту.

5.2.7 Ручне відновлення (ДВ-1)

5.2.7.1 Послуга "Відновлення після збоїв" рівня ДВ-1 дозволяє забезпечити доступність послуг і ресурсів ІТС ОДС ОР шляхом переведення ІТС ОДС ОР у відомий захищений стан після відмови або переривання обслуговування.

5.2.7.2 Множиною типів відмов ІТС ОДС ОР і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки є:

– відмова програмних складових ІТС ОДС ОР внаслідок порушення цілісності або видалення їх складових (файлів, що виконуються, програмних бібліотек тощо);

– порушення цілісності або видалення об'єктів захисту {Д_ПСД}, {Д_СІ}, {Д_ДОВ};

– помилки файлової системи;

– помилки БД;

– відмова технічних засобів зі ІТС ОДС ОР.

5.2.7.3 Відмови, що стосуються об'єктів захисту {Д_ПСД}, {Д_СІ}, {Д_ДОВ} мають усуватися із використанням резервних копій. Відмови програмних складових ІТС ОДС ОР (до яких відноситься політика послуги) мають усуватися шляхом їх повторної інсталяції або заміні пошкоджених програмних складових з еталонної копії.

5.2.7.4 Відмови, пов'язані з помилками файлової системи та БД мають усуватися запуском відповідних утиліт.

5.2.7.5 Після відмови об'єктів, що їх стосується послуга, КЗЗ ІТС ОДС ОР має перевести відповідні об'єкти до стану, із якого повернути його до нормального функціонування може тільки К_АБ чи К_АС. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ІТС ОДС ОР до нормального функціонування.

5.2.8 Модернізація (ДЗ-1)

5.2.8.1 КЗЗ ІТС ОДС ОР має надавати можливість додавання або заміни однієї з РС, одного з елементів комунікаційного обладнання.

5.2.8.2 КЗЗ ІТС ОДС ОР має надавати можливість оновлення ОС, ПЗ КЗІ, ФПЗ, ПЗ антивірусного захисту, СКБД, ПЗ загального призначення.

5.2.8.3 КЗЗ ІТС ОДС ОР має надавати можливість оновлення засобів КЗІ на такі самі або аналогічні засоби, за умови наявності у останніх експертного висновку Адміністрації Держспецзв'язку у сфері КЗІ та при дотриманні вимог визначених у ТЗ та технічних умовах на засіб КЗІ, що проходитиме випробування в ході державної експертизи КСЗІ в ІТС ОДС ОР.

5.2.8.4 КЗЗ ІТС ОДС ОР має надавати можливість оновлення МЕ, ПЗ антивірусного захисту на аналогічні, за умови наявності у останніх експертного висновку Адміністрації Держспецзв'язку у сфері ТЗІ.

5.2.8.5 Право на модернізацію повинні мати користувачі з ролями К_АС, К_АБ. Розподіл їх обов'язків при модернізації повинен бути уточнений на етапі технороботочого проектування.

5.2.8.6 Порядок модернізації та здійснення випробувань після модернізації складу компонентів ІТС ОДС ОР має бути визначений у інструкції (порядку) модернізації.

5.2.8.7 Модернізація не повинна призводити до повторної інсталяції компонентів ІТС ОДС ОР, переривання виконання КЗЗ ІТС ОДС ОР функцій захисту чи проведення додаткової державної експертизи КСЗІ в ІТС ОДС ОР

5.2.8.8 На етапі техноробочого проектування має бути уточнено склад компонентів до яких відноситься політика послуги.

5.2.9 Захищений журнал (НР-2)

5.2.9.1 Послуга "Реєстрація" рівня НР-2 дозволяє контролювати небезпечні для ІТС ОДС ОР дії та забезпечити спостережність за діями користувачів.

5.2.9.2 КЗЗ ІТС ОДС ОР згідно із політикою реєстрації має реєструвати такі події, що мають безпосереднє відношення до безпеки:

– вхід/вихід або спроби входу/виходу в/із системи користувачами будь-яких категорій;

– реєстрація та видалення користувачів будь-якої категорії в системі;

– зміна атрибутів або прав доступу користувача будь-якої категорії чи процесу та дії, що призвели до цього;

– отримання або намагання отримання доступу користувачем чи процесом будь-якої категорії до будь-яких захищених процесів і об'єктів ІТС ОДС ОР та дії над ними;

– модифікація або спроби модифікації захищених процесів і об'єктів ІТС ОДС ОР, у тому числі факти та спроби порушення цілісності КЗЗ;

– спроби використання обчислювальних ресурсів ІТС з перевищенням встановлених квот;

– викриття порушення цілісності чи відмова компонентів, що входять до складу ІТС ОДС ОР;

– отримання з інших ІТС відомостей;

– факти використання послуги "ЦО-1".

5.2.9.3 Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача (об'єкта-користувача чи процесу), програмного засобу, що мали відношення до кожної зареєстрованої події.

5.2.9.4 Користувач з роллю К_АБ, К_АС, К_АБД повинні мати в своєму розпорядженні засоби безпечної передачі журналів з серверів, перегляду і аналізу журналу реєстрації.

5.2.9.5 КЗЗ ІТС ОДС ОР повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Має бути заборонено редагування вмісту журналів реєстрації. Операції очищення (принаймні останнього) також мають відслідковуватися із використанням журналу реєстрації.

5.2.9.6 Перелік подій, які підлягають реєстрації, може бути розширений на етапі техноробочого проектування.

5.2.10 Одиночна ідентифікація та автентифікації (НИ-2)

5.2.10.1 Послуги "Ідентифікація та автентифікація" рівня НИ-2 дозволяють КЗЗ ІТС ОДС ОР визначити і перевірити особистість користувача, що намагається одержати доступ до функцій та інформації, які надаються компонентами ІТС ОДС ОР.

5.2.10.2 Політика послуги НИ-2 відноситься до користувачів з ролями К_АБ, К_АС, К_АБД, К_ВК при їх ідентифікації в ІТС ОДС ОР з метою отримання доступу до наданих їм функцій.

5.2.10.3 КЗЗ ІТС ОДС ОР має надавати доступ до функцій та інформації ІТС ОДС ОР, що запитує користувач, лише після успішного проходження процедури ідентифікації та автентифікації на підставі множини атрибутів, якими характеризуються суб'єкти доступу, що наведені у таблиці. 5.2.

5.2.10.4 Перш ніж дозволити будь-якому користувачу виконувати будь-які інші контрольовані КЗЗ дії, КЗЗ ІТС ОДС ОР повинен ідентифікувати та автентифікувати цього користувача з використанням атрибутів, якими характеризуються суб'єкти доступу, що наведені у таблиці. 5.2.

5.2.10.5 КЗЗ ІТС ОДС ОР не повинен передавати та/або зберігати паролі у відкритому вигляді. Замість паролю має використовуватися результат (геш-значення) його перетворення із застосуванням односпрямованих криптографічних функцій – функцій гешування.

5.2.10.6 КЗЗ ІТС ОДС ОР повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

5.2.11 Однонаправлений достовірний канал (НК-1)

5.2.11.1 КЗЗ ІТС ОДС ОР має гарантувати користувачам можливість безпосередньої взаємодії з ним.

5.2.11.2 КЗЗ ІТС ОДС ОР повинен використовувати механізми КЗІ для захисту даних автентифікації, які передаються від користувачів К_АБ, К_АС, К_АБД, К_ВК при підключені до ІТС ОДС ОР.

5.2.11.3 Встановлення достовірного зв'язку між користувачем і КЗЗ ІТС ОДС ОР, повинно здійснюватися з використанням захищеного (від перехоплення чи підміни) механізму введення користувачем свого паролю.

5.2.11.4 Політика послуги відноситься до користувачів К_АБ, К_АС, К_АБД, К_ВК.

5.2.11.5 Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації користувачів, до яких відноситься політика послуги. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

5.2.12 Розподіл обов'язків адміністраторів (НО-2)

5.2.12.1 Послуга "Розподіл обов'язків" рівня НО-2 дозволяє зменшити потенційний збиток від навмисних або помилкових дій користувачів і обмежити авторитарність керування.

5.2.12.2 КЗЗ ІТС ОДС ОР повинен підтримувати:

– адміністративні ролі (К_АБ, К_АС, К_АБД);

– користувальницькі ролі (К_ВК).

5.2.12.3 Функції, притаманні кожній з ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

5.2.12.4 Користувач ІТС ОДС ОР повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

5.2.13 КЗЗ з гарантованою цілісністю (НЦ-2)

5.2.13.1 Доменом КЗЗ ІТС ОДС ОР повинен бути серверний сегмент ІТС ОДС ОР (по суті внутрішня мережа ІТС). Межею домену ІТС ОДС ОР є зовнішній інтерфейс міжмережевого екрана.

5.2.13.2 У якості механізму забезпечення цілісності компонентів, що входять до складу КЗЗ ІТС ОДС ОР мають використовуватися механізми захисту, що використовуються для реалізації розподілення доменів у міжмережевому екрані, комутаторах, КЗЗ ОС РС, КЗЗ ОС серверів, ФПЗ.

5.2.13.3 КЗЗ ІТС ОДС ОР повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

5.2.13.4 За допомогою організаційних заходів має бути забезпечено неможливість завантаження серверів та РС зі складу комплексу технічних засобів ІТС ОДС ОР із зовнішніх носіїв або через мережевий інтерфейс.

5.2.13.5 На етапі технічного проектування обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ ІТС ОДС ОР і всі запити на доступ до захищених об'єктів контролюються КЗЗ ІТС ОДС ОР, можуть бути уточнені.

5.2.14 Самотестування при старті (НТ-2)

5.2.14.1 КЗЗ ІТС ОДС ОР повинен перевіряти і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КЗЗ ІТС ОДС ОР.

5.2.14.2 Процедурами, що мають використовуватися для оцінки правильності функціонування КЗЗ ІТС ОДС ОР є:

– тестування на предмет вірусного зараження;

– перевірка коректності конфігураційних файлів окремих програмних засобів;

– тестування правильності криптографічних перетворень, що реалізовані у засобах КЗІ зі складу КЗЗ ІТС ОДС ОР.

5.2.14.3 КЗЗ ІТС ОДС ОР має бути здатним виконувати набір тестів з метою оцінки правильності функціонування. Тести повинні виконуватися при запуску та за запитом користувача з роллю К_АБ, К_АС, К_АБД або іншого уповноваженого користувача. Тести повинні виконуватися при старті та за запитом відповідного адміністратора.

5.2.14.4 Перелік процедур та тестів, що призначені для реалізації послуги може бути уточнений на етапі технічного проектування.

5.2.15 Автентифікація вузла (НВ-1)

5.2.15.1 Послуга "Ідентифікація і автентифікація при обміні" рівня НВ-1 дозволяє КЗЗ ІТС ОДС ОР ідентифікувати (встановити і перевірити ідентичність) іншого КЗЗ і забезпечити іншому КЗЗ можливість ідентифікувати себе, перед початком взаємодії.

5.2.15.2 Політика послуги відноситься до ІТС ОДС ОР, ІТС ОДС ЦР та джерел оновлення ПЗ. У якості атрибутів повинні використовуватись сертифікати відкритих ключів. У якості процедур взаємної ідентифікації при ініціалізації обміну даними з ІТС ОДС повинні використовуватись протоколи взаємної ідентифікації та автентифікації на основі КЕП.

5.2.15.3 КЗЗ ІТС ОДС ОР, перш ніж почати обмін даними з КЗЗ ІТС ОДС ЦР, повинен ідентифікувати і автентифікувати зазначені КЗЗ з використанням захищеного механізму.

5.2.15.4 КЗЗ ІТС ОДС ОР, перш ніж оновити ПЗ, повинен ідентифікувати та автентифікувати джерело оновлення ПЗ (ІТС виробника, з якої отримано оновлення).

5.2.15.5 Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації протоколу на основі КЕП.

5.2.16 Автентифікація відправника з підтвердженням (НА-2)

5.2.16.1 Послуга "Автентифікація відправника" рівня НА-2 дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений та/або відправлений певним користувачем.

5.2.16.2 Політика послуги має відноситися до:

– користувачів К_АБ, К_АС, К_АБД, К_ВК та об'єкта захисту {Д_ЕД};

– користувачів К_ВК та об'єкта захисту {Д_ЄДРПОУ}.

5.2.16.3 Атрибутом, що дозволяє однозначно встановити, що об'єкт був створений (відправлений) певним користувачем, має бути КЕП.

5.2.16.4 Перелік об'єктів захисту може бути розширений на етапі техноробочого проектування.

5.2.16.5 Атрибутами користувачів на яких поширюється політика послуги має бути особистий ключ КЕП (електронної печатки для ФПЗ та процесів) та сертифікат відкритого ключа.

5.2.16.6 Процедурою, що дозволяє однозначно встановити, що об'єкт захисту був створений (відправлений) певним користувачем (чи процесом), є перевірка КЕП цих даних. Засоби КЗІ, які використовуються для реалізації функцій КЕП, повинні мати чинний експертний висновок в сфері КЗІ. Для забезпечення можливості однозначного підтвердження належності об'єкта незалежною третьою стороною, у складі КЗЗ інших ІТС, ІТС ОДС ОР при формуванні та перевірянні КЕП мають використовуватися надійні засоби КЕП та посилені сертифікати відкритих ключів.

5.2.16.7 У якості незалежної третьої сторони має виступати кваліфікований надавач електронних довірчих послуг.

6 ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ

6.1 Проектна документація на комплексну систему захисту інформації повинна включати:

– пояснювальну записку технoробочого проекту КСЗІ в ІТС ОДС ОР;

– план захисту інформації ІТС ОДС ОР(сукупність документів) у якому має бути визначено:

– перелік інформації, що підлягає автоматизованому обробленню в ІТС ОДС ОР та потребує захисту;

– опис моделі загроз для інформації, оброблюваної в ІТС ОДС ОР та моделі порушника;

– опис політики безпеки інформації інформації в ІТС ОДС ОР;

– перелік типової організаційно-розпорядчої документації КСЗІ.

– методика розгортання організаційно-технічного рішення КСЗІ ІТС ОДС ОР на реальному об'єкті;

– методика випробувань організаційно-технічного рішення КСЗІ ІТС ОДС ОР, при її розгортанні на реальному об'єкті.

6.2 До складу документації технoробочого проекту повинні входити: основні технічні рішення щодо побудови КСЗІ у ІТС ОДС ОР; опис складу КЗЗ; опис функціонування механізмів захисту; способи реалізації послуг безпеки; основні правила експлуатації КЗЗ.

6.3 Експлуатаційна документація КСЗІ кожного ІТС ОДС ОР повинна включати:

1) типове положення про службу захисту інформації в ІТС;
2) настанови, інструкції та правила:
– Інструкція про порядок введення в експлуатацію КСЗІ;
– Інструкція про порядок модернізації компонентів ІТС ОДС ОР;
– Правила видачі, вилучення та обліку персональних ідентифікаторів;
– Інструкція про організацію контролю за функціонуванням КСЗІ;
– Інструкції з використання засобів КЗІ (які постачаються разом із засобами КЗІ);
– Посадова інструкція адміністратора безпеки;
– Посадова інструкція системного адміністратора;
– Посадова інструкція адміністратора БД;
– Посадова інструкція внутрішнього користувача;
– Інструкція щодо взаємодії з іншими ІТС;
– Інструкція з антивірусного захисту.

6.4 Під час розроблення цих документів дозволяється поєднувати кілька з них у вигляді окремих розділів одного документу.

6.5 Остаточний склад і зміст експлуатаційної документації мають бути уточнені на етапі розробки технoробочого проекту.

7 ЕТАПИ ВИКОНАННЯ РОБІТ

7.1 Узагальнені етапи виконання робіт зі створення КСЗІ ІТС ОДС ОР наведені у таблиці 7.1

Таблиця 7.1 – Етапи виконання робіт

Стадія	Етапи робіт	Результат роботи
1 Технічне завдання	1.1. Розробка та погодження технічного завдання на створення типового організаційно-технічного рішення КСЗІ в ІТС ОДС ОР	Затверджене ТЗ на створення типового організаційно-технічного рішення КСЗІ в ІТС ОДС ОР
2 Технороботчий проект	2.1 Розробка технічного проекту організаційно-технічного рішення для КСЗІ в ІТС ОДС ОР відповідно до вимог ТЗ на КСЗІ в ІТС ОДС ОР. 2.2 Розробка робочої та експлуатаційної документації організаційно-технічного рішення (у тому числі документації КСЗІ ІТС ОДС ОР)	1. Пояснювальна записка до технічного проекту організаційно-технічного рішення для КСЗІ в ІТС ОДС ОР відповідно до вимог ТЗ на КСЗІ в ІТС ОДС ОР. 2. Робоча та експлуатаційна документація організаційно-технічного рішення (у тому числі документація КСЗІ ІТС ОДС ОР)
3 Введення в дію та перевірка працездатності КСЗІ	3.1 Реалізація (впровадження) заходів щодо організаційно-технічного рішення. 3.2 Розробка і затвердження "Програми і методики попередніх випробувань організаційно-технічного рішення". 3.3 Проведення попередніх випробувань організаційно-технічного рішення. 3.4 Корегування документації організаційно-технічного рішення (у тому числі документації КСЗІ ІТС ОДС ОР)	1. КЗЗ, реалізований і інстальований в організаційно-технічному рішенні. 2. Програма і методика попередніх випробувань організаційно-технічного рішення. 3. Протокол попередніх випробувань організаційно-технічного рішення. 4. Дороблена документація організаційно-технічного рішення (у тому числі документація КСЗІ ІТС ОДС ОР).
4 Державна експертиза	4.1 Супровід експертних робіт	Експертний висновок на організаційно-технічне рішення на КСЗІ в ІТС ОДС ОР

7.2 Впровадження КСЗІ в ІТС ОДС ОР на реальному об'єкті передбачає здійснення таких основних етапів:

– розгортання організаційно-технічного рішення для КСЗІ в ІТС ОДС ОР в ІТС кожного територіального управління у відповідності до документу "Методика розгортання організаційно-технічного рішення для КСЗІ в ІТС ОДС ОР на реальному об'єкті";

– випробування КСЗІ в ІТС ОДС ОР у відповідності до документу "Методика випробувань КСЗІ в ІТС ОДС ОР, при її розгортанні на реальному об'єкті";

– оформлення та затвердження акту завершення робіт зі створення КСЗІ в ІТС ОДС ОР відповідно до вимог документу "Типовий акт завершення робіт зі створення КСЗІ в ІТС ОДС ОР на реальному об'єкті" та оформлення формуляру ІТС ОДС ОР відповідно до вимог документу "Типовий формуляр ІТС ОДС ОР на реальному об'єкті";

– надсилання затвердженого керівником територіального управління-власника ІТС ОДС ОР акту завершення робіт зі створення КСЗІ в ІТС ОДС ОР до Адміністрації Держспецзв'язку;

– на підставі розгляду затвердженого акту завершення робіт зі створення КСЗІ в ІТС ОДС ОР та на підставі Експертного висновку на організаційно-технічне рішення для КСЗІ в ІТС ОДС ОР Адміністрація Держспецзв'язку приймає рішення про можливість видачі Атестату відповідності КСЗІ в ІТС ОДС ОР;

– після отримання Атестату відповідності КСЗІ в ІТС, територіальне управління вводить свою ІТС ОДС ОР у промислову експлуатацію.

8 ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЗ

Зміни затвердженого ТЗ на створення КСЗІ, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку, що і основний документ.

9 ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ КСЗІ

9.1 Метою випробувань є визначення відповідності створеного організаційно-технічного рішення для КСЗІ в ІТС ОДС ОР вимогам ТЗ для подальшого його розгортання в ІТС кожного обласного відділу Держстату.

9.2 Проводяться наступні види випробувань організаційно-технічного рішення: попередні, державна експертиза. За результатами попередніх випробувань складається протокол, у якому зазначаються результати випробувань і дається висновок щодо можливості представлення організаційно-технічного рішення на державну експертизу.

9.3 Державна експертиза організаційно-технічного рішення здійснюється відповідно до "Положення про державну експертизу в сфері технічного захисту інформації", яке затверджено наказом Адміністрації Держспецзв'язку від 16.05.2007 р. №93 (із змінами затвердженими наказом Адміністрації Держспецзв'язку).

9.4 Для забезпечення можливості вводу КСЗІ в ІТС кожного обласного відділу Держстату у промислову експлуатацію необхідно здійснити етапи робіт, які зазначені в п.7.2.

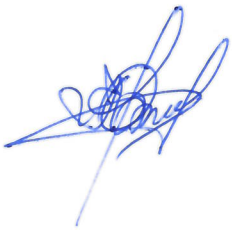
10 ВИМОГИ ІЗ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОНАННІ РОБІТ

Перелік осіб, які можуть бути ознайомлені з матеріалами проектної й експлуатаційної документації КСЗІ, визначається замовником та розробником. Порядок доступу цих осіб до матеріалів установлюється відповідно до діючих нормативних документів України.

Обґрунтування розміру бюджетного призначення та очікуваної вартості предмета закупівлі

Розмір бюджетного призначення для надання послуг щодо впровадження КСЗІ відповідає розрахунку видатків до кошторису Держстату на 2021 рік (загальний фонд) за КПКВК 0414010 "Керівництво та управління у сфері статистики" по КЕКВ 2240 "Оплата послуг (крім комунальних)".

Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених для Державної служби статистики Кошторисом на 2021 рік для апарату Держстату за бюджетною програмою КПКВК 0414010 "Керівництво та управління у сфері статистики" по КЕКВ 2240 "Оплата послуг (крім комунальних)" відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18 лютого 2020 року № 275. У зв'язку з обмеженою конкуренцією на ринку послуг, які є предметом закупівлі, що підтверджено експертним висновком щодо наявності підстав застосування переговорної процедури закупівлі на підставі абзацу четвертого пункту 2 частини другої статті 40 Закону України "Про публічні закупівлі", а саме: послуги можуть бути надані виключно певним суб'єктом господарювання за наявності одного з випадків, а саме: відсутність конкуренції з технічних причин, тому було застосовано метод розрахунку очікуваної вартості на підставі ціни закупівлі аналогічних послуг, здійсненої Держстатом у 2020 році. Очікувана вартість послуг визначена на рівні ціни договору, укладеного у 2020 році, з урахуванням збільшеного обсягу послуг, що надаються.

Завідувач сектору захисту
інформації Держстату  Олег ЧЕРНЕНКО