ТЕХНІЧНІ ВИМОГИ

до закупівлі послуг з модернізації комплексної системи захисту інформації інформаційно-комунікаційної системи «Єдина інформаційна система соціальної сфери» Міністерства соціальної політики України

1. Перелік термінів, визначень, скорочень та абревіатур

Термін	Пояснення
API (Application Programming Interface)	Прикладний інтерфейс програмування
BI	Business intelligence — це збір, зберігання і аналіз даних що утворюються
Front-Office	Група структурних підрозділів відповідальних за безпосередню взаємодію з отримувачами соціальної підтримки (структурні підрозділи з питань соціального захисту населення виконавчих органів сільської, селищної, міської ради, районних в містах Києві та Севастополі державних адміністрацій, центри надання адміністративних послуг)
Автентифікація	Електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних
Адміністратор ЄІССС	Організація, установа, підприємство, що забезпечує організаційні та технічні аспекти функціонування ЄІССС. На етапі експерименту тимчасовим Адміністратором ЄІССС визначений Пенсійний фонд України
АРМ	Автоматизоване робоче місце
БД	База даних
Діловий процес	Це комплекс видів діяльності, які визначаються точками «входу» і «виходу» та використовують організаційні ресурси з метою створення цінності товарів/послуг для споживача
Державні інформаційні ресурси	систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень

Термін	Пояснення
Держспецзв’язку	Державна служба спеціального зв’язку та захисту інформації України
Заявник	Фізична особа або її представник, що звертається щодо соціальної підтримки до Front-Office , в тому числі шляхом взаємодії з ними в електронній формі через Єдиний державний веб-портал електронних послуг «Портал Дія», офіційний веб-сайт Мінсоцполітики, інтегровані з ним інформаційні системи органів виконавчої влади та органів місцевого самоврядування, а також інформаційні системи Мінсоцполітики
Звернення	Будь-яке звернення заявника щодо вирішення питань, які стосуються послуг, що зареєстроване в Системі (консультація споживача щодо процедури отримання послуг, запис на прийом, надання заявнику інформації щодо замовлених послуг, прийом заявника спеціалістом Front-офісу, подача заявником повного/неповного пакету документів на прийомі, замовлення заявником послуги в електронній формі та ін.)
Зовнішня система	Апаратно-програмний комплекс, який не є складової Системи
ЄДАРП	Єдиний державний автоматизований реєстр осіб, які мають право на пільги створений для забезпечення єдиного державного обліку фізичних осіб, які мають право на пільги за соціальною ознакою згідно із законами України, отримують пільги, передбачені для педагогічних, медичних, фармацевтичних працівників, працівників бібліотек, музеїв, спеціалістів із захисту рослин та працівників культури в сільській місцевості і селищах міського типу (далі - пільговики), отримують соціальні стипендії, державну допомогу постраждалим учасникам масових акцій громадського протесту та членам їх сімей
ЄІССС	Єдина інформаційна система соціальної сфери.
ЄСР	Єдиний соціальний реєстр
Ідентифікаційні дані особи	Унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи
Ідентифікація особи	Процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи
ІКС	Інформаційно-комунікаційна система

Термін	Пояснення
ІКС «ЄІССС»	інформаційно-комунікаційна система «Єдина інформаційна система соціальної сфери»
ІКІС ПФУ	Інтегрована комплексна інформаційна система Пенсійного фонду України
Інституції соціального захисту	Мінсоцполітики, установи та організації, що належать до сфери управління Мінсоцполітики, Пенсійний фонд України та його територіальні органи, Нацсоцслужба та її територіальні органи, виконавча дирекція Фонду соціального страхування України та її робочі органи, Фонд соціального захисту осіб з інвалідністю та його територіальні відділення, місцеві органи виконавчої влади, органи місцевого самоврядування
Інформаційна система Міністерства.	Будь-яка інформаційна система, що знаходиться в експлуатації Мінсоцполітики
КЗЗ	Комплекс засобів захисту
КЗІ	Криптографічний захист інформації
КСЗІ	Комплексна система захисту інформації
Користувач	Працівник інституції соціального захисту, наділений правами на користування системою, адміністратор центру надання адміністративних послуг, користувач особливої категорії — адміністратор системи та адміністратор безпеки системи. Рівень доступу до даних та інформації в системі встановлюється відповідно до посадових повноважень користувача
Мінсоцполітики	Міністерство соціальної політики України
НСД	Несанкціонований доступ
ОС	Операційна система
ОСЗН	Орган соціального захисту населення
Органи державної влади	Міністерства та інші центральні органи виконавчої влади (служби, агентства, інспекції), Центральні органи виконавчої влади зі спеціальним статусом (Антимонопольний комітет України, Фонд державного майна, Державний комітет з телебачення та радіомовлення), а також їх територіальні органи, місцеві державні адміністрації (обласні і районні державні адміністрації, Київська міська державна адміністрація)
ТГ	Територіальна громада

Термін	Пояснення
ПЗ	Програмне забезпечення
Підсистема	Сукупність елементів, що представляють логічно завершену частину Системи, що відповідають за реалізацію визначеного напряму автоматизації
Портал «ДІЯ»	Єдиний державний веб-портал електронних послуг «Портал Дія»
ПФУ	Пенсійний фонд України
РЗО	Реєстр застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування
РС	Робоча станція
Система	ЄІССС
СКБД	Система керування базами даних
Стратегія	Стратегія цифрової трансформації соціальної сфери, схвалена розпорядженням Кабінету Міністрів України від 28.10.2020 № 1353-р
Споживач	Особа, якій надаються / яка має право на будь-які соціальні виплати, пільги, послуги, заходи, що передбачені для громадян законодавством і забезпечуються інституціями соціального захисту за рахунок коштів державного та місцевих бюджетів, Пенсійного фонду України, фондів загальнообов'язкового державного соціального страхування, міжнародної технічної допомоги та інших джерел, не заборонених законодавством
ТЗ, Технічне завдання	Вихідний документ для проєктування, у відповідності до якого проводиться виготовлення, приймання при введенні в дію та експлуатація відповідного об'єкту
Трембіта	Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», держателем якої є Мінцифри
ЦБІ	Централізований банк даних з проблем інвалідності
ЦНАП	Центр надання адміністративних послуг
ЦОД	Центр обробки даних

2. Загальні вимоги

При модернізації комплексної системи захисту інформації (далі − КСЗІ) повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки

відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного та криптографічного захисту інформації.

Повне найменування КСЗІ та її умовне позначення

Повне найменування КСЗІ – комплексна система захисту інформації інформаційно-комунікаційної системи «Єдина інформаційна система соціальної сфери» (далі – ІКС «ЄІССС»).

Скорочена назва – КСЗІ в ІКС «ЄІССС».

ЄІССС – єдина комплексна інформаційно-аналітична система соціальної сфери, що призначена для накопичення, зберігання та автоматизованого оброблення інформації щодо соціального захисту населення, створена з урахуванням новітніх інформаційних та управлінських технологій, єдиних сучасних стандартів якості обслуговування заявників, можливостей вироблення ефективних організаційних і структурних рішень. Держателем Єдиної інформаційної системи соціальної сфери є Мінсоцполітики.

Мінсоцполітики здійснює заходи з модернізації ЄІССС в частині розробки соціального веб-порталу, який, шляхом інформаційного обміну з базою даних (далі – БД) ЄІССС, забезпечує збір та обробку даних користувачів з метою надання послуг в сфері соціального захисту для отримувачів різних видів соціальної підтримки (фізичних або юридичних осіб різних форм власності). Соціальний веб-портал надає відповідний веб-інтерфейс для формування запитів на отримання соціальних послуг для користувачів соцпорталу (фізичні або юридичні особи, які створили власний кабінет в ЄІССС) та кейс-менеджерів (представники контролюючих органів, які здійснюють збір вхідної інформації для реєстрації заяв отримувачів різних видів соціальної підтримки, шляхом проведення опитувань та занесення даних в БД ІКС «ЄІССС» через виділений кабінет кейс-менеджеру).

Модернізація ІКС «ЄІССС» проводиться з метою індивідуального та захищеного підключення зовнішніх користувачів до ЄІССС за допомогою розгортання електронних кабінетів користувачів в окремо виділеному веб-порталі, ізольованих від загального сховища даних ЄІССС (БД ІКС «ЄІССС») та інформаційних ресурсів інших зовнішніх користувачів.

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІКС «ЄІССС» у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації, зокрема:

– організаційно-правові заходи, які реалізуються поза обчислювальною системою ІКС «ЄІССС»;

– інженерно-технічні заходи, що реалізуються поза обчислювальною системою ІКС «ЄІССС»;

– апаратні, програмно-апаратні та програмні засоби:

- захисту від несанкціонованого доступу (далі – НСД);
- криптографічного захисту інформації (далі – КЗІ);
- забезпечення доступності інформації, що обробляється в ІКС «ЄІССС».

3. Опис ІКС «ЄІССС»

Для виконання завдань проєкту в ході його реалізації

– створені основні загальні підсистеми ЄІССС, визначені Стратегією, а саме:

- Єдиний соціальний реєстр.
- Реєстр надавачів та отримувачів соціальних послуг.
- Підсистема «Електронний бюджет».
- Підсистема «Соціальне казначейство».

- Підсистема верифікації отримувачів соціальної підтримки.
- Підсистема обміну даними із суб'єктами інформаційної взаємодії.
- Підсистема «Єдиний соціальний процесинг».
- Підсистема ретроконверсії.
- Підсистема дистанційного інформування.
- Аналітична підсистема.
- Адміністративна підсистема.
- Підсистема ведення довідників та реєстрів загального призначення.
- Підсистема «Єдиний електронний архів соціальної сфери».
- Підсистема «Житлові субсидії».
- Підсистема «Державні допомоги, винагороди та компенсації».
- Підсистема «Соціальні послуги».
- Підсистема «Дозвільні документи та довідки».
- Підсистема «Банк даних про дітей».
- Підсистема «Облік малозабезпечених сімей».
- Підсистема «ЄДАРП».
- Підсистема «ЕІБД ВПО».

– розробляються в рамках модернізації:

- електронні кабінети користувачів соціального порталу (громадянина, надавачів соціальних послуг, органів виконавчої влади, кейс-менеджера, міжвідомчої взаємодії тощо), які надають відповідний веб-інтерфейс надання соціальних послуг. Доступ користувачів до виділених кабінетів надається за кваліфікованим електронним підписом (далі – КЕП);
- електронні кабінети кейс-менеджерів, які надають відповідний веб-інтерфейс для внесення інформації користувачів необхідної для отримання соціальних послуг. Доступ кейс-менеджерів до виділених кабінетів надається за КЕП;
- веб-портал BI, що містить загальнодоступну публічну інформацію (довідкова інформація, інтерфейси для пошуку даних статистичні відомості тощо);
- резервна копія ЄІССС, яка розгорнута в хмарному середовищі та працює в режимі дублювання (кластеризації) разом із наземним рішенням ЄІССС, що забезпечує стале функціонування, зниження навантаження та збільшення продуктивності Системи;
- підсистема адміністрування ІКС «ЄІССС», яка забезпечує єдину інфраструктуру керування інформаційними потоками системи віртуалізації ІКС «ЄІССС» та ІКС в цілому.

Для забезпечення безперервності процесу автоматизації надання соціальної підтримки при переході від діючих інформаційних систем до ЄІССС потрібно забезпечити інтеграцію ЄІССС в ізольоване та відокремлене від ІКС «ЄІССС» хмарне середовище Microsoft Azure, що забезпечує додатковий захист конфіденційної інформації (персональні дані користувачів, державні інформаційні ресурси). В додаткових підсистемах ІКС «ЄІССС» (електронні кабінети користувачів соціального порталу, електронні кабінети кейс-менеджерів, веб-портал BI, що містить загальнодоступну публічну інформацію, підсистема адміністрування ІКС «ЄІССС») що розробляються під час модернізації, заборонено зберігання конфіденційної інформації зовнішніх користувачів.

Веб-портал ІКС «ЄІССС» повинен взаємодіяти з зовнішніми користувачами використовуючи функціонал веб-браузерів останньої версії.

Під час впровадження ІКС «ЄІССС» забезпечується інтеграція з зовнішніми системами виключно за погодженими протоколами інформаційної взаємодії.

ЄІССС реалізує інформаційну взаємодію при наявності відповідних нормативних актів, що обумовлюють використання та правила отримання інформації з державних реєстрів та баз даних та наявності відповідних прикладних програмних інтерфейсів (API) з наступними підсистемами та відомствами (в тому числі за допомогою системи Трембіта):

– Мінсоцполітики (міграція даних з ЦБІ).

– ПФУ (онлайн запити/відповіді для взаємодії з РЗО).

– Мінцифри (онлайн запити/відповіді для Порталу «Дія»).

– ДПС (онлайн запити/відповіді).

– Мінюст (онлайн запити/відповіді).

– Інші державні реєстри та інформаційні системи центральних органів виконавчої влади України.

4. Опис архітектури ІКС «ЄІССС»

В узагальненому вигляді ІКС «ЄІССС» складається з трьох основних рівнів:

– система віртуалізації ІКС «ЄІССС» (серверне та мережеве обладнання, з відповідним ПЗ, що забезпечує передачу даних користувачів соціального порталу та кейс-менеджерів до виділеної ізольованої БД ІКС «ЄІССС»), розгортання якого передбачене у хмарному середовищі Microsoft Azure;

– технологічний майданчик ІКС «ЄІССС» (серверне та мережеве обладнання, з відповідним ПЗ, що забезпечують реалізацію покладених на ІКС «ЄІССС» функцій), розгортання якого проведене в рамках створення КСЗІ ІКС «ЄІССС»;

– сегмент адміністрування ІКС «ЄІССС» (мережа що здійснює підтримку функціонування системи віртуалізації ІКС «ЄІССС» та розміщена на базі технологічного майданчику ІКС «ЄІССС»).

Технологічний майданчик ІКС «ЄІССС» являє собою наземне рішення ЄІССС.

Архітектурно програмне забезпечення ЄІССС побудоване як трирівнева централізована WEB-орієнтована система, що включає наступні компоненти:

– сервери БД (основний та резервні), на яких функціонує централізована БД, яка виконує зберігання та санкціоноване надання інформації, а також реалізує певну частину бізнес-логіки засобами СКБД;

– сервери додатків, які реалізують частину бізнес та презентаційної логіки, функції обміну з іншими системами, у т. ч. забезпечують роботу Web-користувачів;

– тонкий (Web) клієнт, який за допомогою Web-інтерфейсу (графічного інтерфейсу користувача – GUI) надає користувачам доступ до даних, що містяться в системі ЄІССС.

Система віртуалізації ІКС «ЄІССС» передбачає розгортання у хмарному середовищі Microsoft Azure наступних підсистем:

- електронні кабінети користувачів соціального порталу;
- електронні кабінети кейс-менеджерів;
- веб-портал BI;
- резервна копія ЄІССС.

ІКС «ЄІССС» являє собою багатокористувацьку мережу, побудовану за змішаною (гібридною) мережевою топологією, з доступом до мережі Інтернет. Ескізний проєкт архітектури ІКС «ЄІССС» та її оточення наведені на рис. 1.

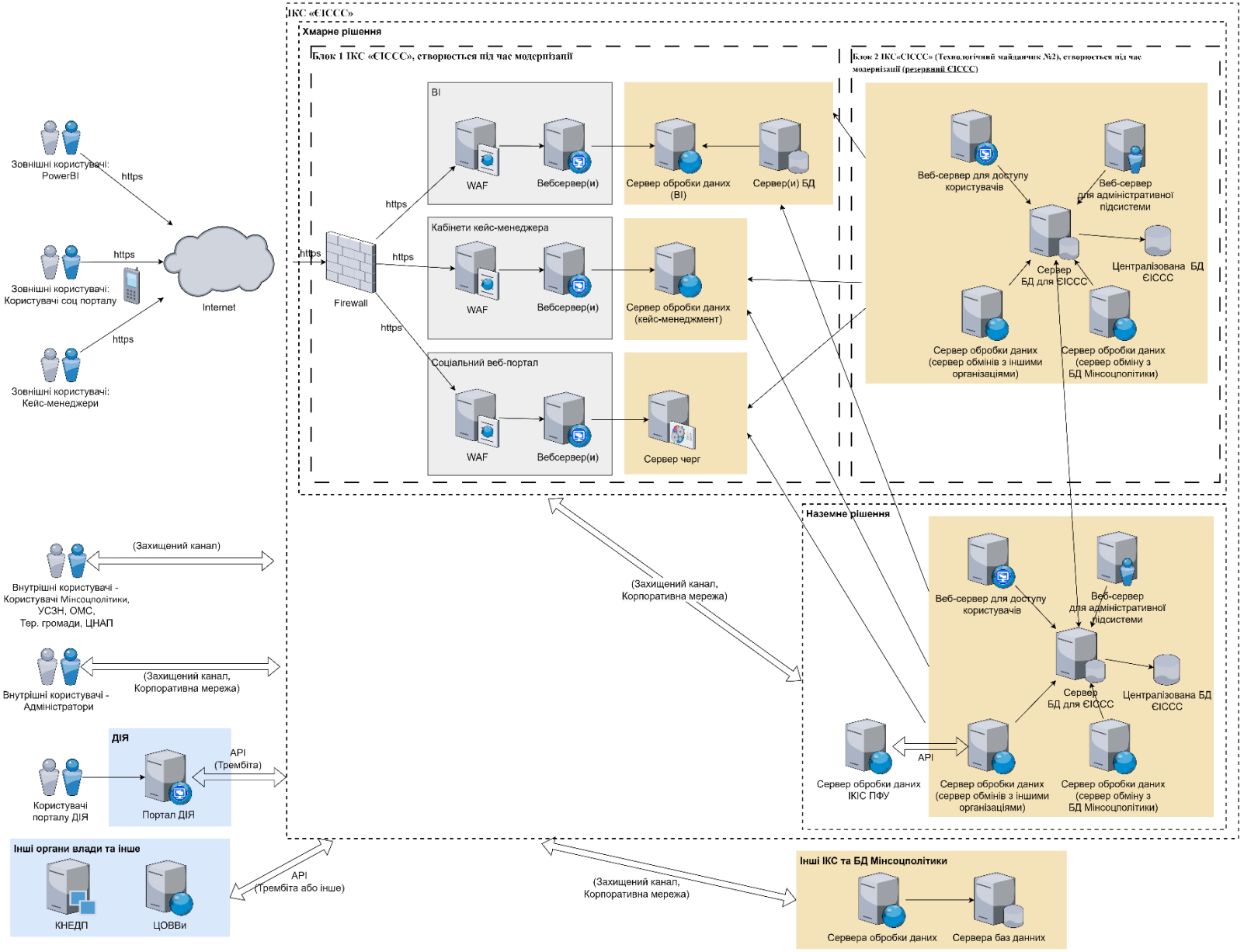

Рис. 4.1 – Ескізний проєкт ІКС «ЄІССС»

Складу ІКС «ЄІССС» передбачено в наступному обсязі:

– сервери віртуалізації;

– сервери БД;

– сервери застосувань/веб-порталу;

– проксі-сервер веб-застосунків;

– міжмережевий екран;

– комутаційне обладнання;

– засоби КЗІ;

– РС адміністраторів;

– Мережевий накопичувач;

– виділені планшети кейс-менеджерів;

– джерела безперебійного живлення;

– тощо.

5. Технічне забезпечення

Апаратне забезпечення технологічного майданчика ІКС «ЄІССС» функціонує на програмно-технічній платформі Пенсійного фонду України, а саме його основного та резервного Центрів обробки даних (далі – ЦОД).

Апаратне забезпечення серверної частини складається з фізичних серверів баз даних, які працюють під управлінням ОС Oracle Linux (версії, сертифікованої для версії СКБД Oracle EE v.12.2.0.1, яка функціонує в ПФУ). Для функціонування СКБД використовуються спеціалізовані апаратні рішення для роботи бази даних, такі як Oracle Exadata X9M-2.

Система віртуалізації ІКС «ЄІССС» повинна функціонувати на програмно-технічній платформі, розгортання якої передбачене у хмарному середовищі Microsoft Azure.

Повинна бути передбачення можливість міграції системи у власний центр обробки даних після завершення робіт з його побудови на території Замовника.

Сегмент адміністрування ІКС «ЄІССС» функціонує на технологічному майданчику ІКС «ЄІССС».

Апаратне забезпечення сегменту адміністрування має складатись з робочих станцій (далі – РС) адміністраторів, внутрішніх користувачів ІКС «ЄІССС» та мережевого обладнання, що призначене для забезпечення обміну інформацією між компонентами системи віртуалізації ІКС «ЄІССС» та сегментом адміністрування на основі топології мережі та правил, що були попередньо задаються адміністратором ІКС «ЄІССС».

АРМ сегменту адміністрування – техніка, яка за своїми апаратними характеристиками дозволяє встановити та підтримати стабільне функціонування системного та спеціального ПЗ ІКС «ЄІССС».

Вимоги до апаратного забезпечення (АРМ):

– для забезпечення роботи АРМ мають використовуватися ліцензійні примірники ПЗ (пропрієтарні або вільнорозповсюджувані) отримані від розробників, їх офіційних дистриб’юторів або завантажені з їх офіційних веб-сайтів;

– обов’язкове використання антивірусного ПЗ, яке регулярно оновлюється та використовується для перевірки всіх з’ємних носіїв, які підключаються до АРМ користувача;

– перевага має надаватися ПЗ, які пройшли експертизу та мають позитивний експертний висновок в сфері ТЗІ;

– має бути забезпечено налаштування BIOS, зокрема встановлено параметри паролю доступу та завантаження виключно з жорсткого диску, відключені непотрібні для роботи системи інтерфейси;

– має бути забезпечено налаштування ПЗ у відповідності до рекомендацій розробника та експертного висновку (за його наявності). В будь-якому разі, має бути забезпечена обов'язкова авторизація в системі з використанням логіну та паролю користувача, реалізовані вимоги до складності паролю та його неповторюваності, блокування облікових записів за умови перевищення кількості невдалих спроб авторизації, контроль цілісності засобів захисту, ведення аудиту події, які мають безпосереднє відношення до безпеки, зокрема вхід/вихід користувачів, зміна налаштувань параметрів безпеки, контроль цілісності компонентів тощо;

– рекомендується встановлювати виключно тільки те ПЗ, яке необхідне для взаємодії з ІКС «ЄІССС» та виконання робочих завдань.

6. Програмне забезпечення

З метою забезпечення ізольованості кабінетів зовнішніх користувачів передбачається розгортання серверів системи віртуалізації у хмарному середові Microsoft Azure, яке забезпечує:

– динамічне розподілення та доступність обчислювальних ресурсів ІКС «ЄІССС»;

– відновлення роботи віртуальних машин ІКС «ЄІССС» в разі відмови одного з віртуальних серверів;

– безперервну доступність віртуальних машин при відмові сервера системи віртуалізації ІКС «ЄІССС» шляхом автоматичної міграції запущених процесів на інший сервер без втрат в обслуговуванні;

– підтримку шаблонів віртуальних машин ІКС «ЄІССС», що надає можливість інсталяції та налаштування машини одразу з шаблону;

– надання засобів моніторингу доступності гостьової ОС та її перезавантаження в разі потреби;

– створення знімків стану віртуальних машин (як працюючої, так і зупиненої), злиття знімків в один та їх видалення без перезавантаження віртуальної машини;

– можливість додавання пристроїв до працюючої віртуальної машини;

– підтримку розширених механізмів оптимізації оперативної пам'яті фізичного хоста (фізичного серверу) (дедуплікація сторінок пам'яті, динамічний розподіл, компресія).

В якості СКБД використовується система Oracle Database Enterprise Edition (версій від 12c та вище).

Сервери веб-порталу (веб-сервери) призначено для обробки запитів до БД ЄІССС, що надходять від адміністраторів та користувачів ІКС «ЄІССС».

Сервери додатків призначено для роботи системного та функціонального ПЗ, яке має реалізовувати технологію логіку обробки інформації в ІКС «ЄІССС».

З метою захисту інформаційних ресурсів ІКС «ЄІССС» передбачається використання міжмережевих екранів (апаратних або віртуальних), які мають забезпечувати взаємодію компонентів віртуальної інфраструктури та базовий захист інфраструктури від зовнішньої взаємодії шляхом використання функцій трансляції мережевих адрес (NAT) та правил брандмауера щодо можливих IP адрес та/або портів взаємодії з зовнішніми системами (Firewall).

З метою виявлення і знешкодження комп'ютерних вірусів і шкідливих програм в режимі реального часу в ІКС «ЄІССС» передбачається інсталяція ПЗ антивірусного захисту.

Взаємодія зовнішнього користувача з ІКС «ЄІССС» має здійснюватися через відкритий інтернет-канал з використанням засобів КЗІ.

Передача конфіденційної інформації, через незахищене середовище (середовище, в якому циркулює інформація, стосовно якої відсутнє підтвердження відповідності захисту від усіх можливих загроз, імовірність прояву яких існує у цьому середовищі) може здійснюватися у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації.

З метою забезпечення конфіденційності та цілісності об'єктів захисту ІКС «ЄІССС», які передаються через незахищене середовище між системою віртуалізації ІКС «ЄІССС» та клієнтськими робочими місцями (інформаційними системами) зовнішніх користувачів, ЄІССС, іншими системами мають використовуватися засоби КЗІ, які мають чинний, позитивний експертний висновок Адміністрації Держспецзв'язку в сфері КЗІ, та, відповідно до нього можуть здійснювати захист конфіденційної інформації у каналах зв'язку.

Конфіденційна інформація, яка міститься у резервних копіях державних інформаційних ресурсів, зберігається у хмарному середовищі Microsoft Azure у зашифрованому вигляді.

Доступ для адміністрування системи віртуалізації ІКС «ЄІССС» має забезпечуватись з використанням засобів КЗІ.

У засобах КЗІ, які застосовуються для захисту/доступу для адміністрування системи віртуалізації ІКС «ЄІССС», зберігання державних інформаційних ресурсів у зашифрованому вигляді на хмарному середовищі Microsoft Azure та передачі конфіденційної інформації, через незахищене середовище, до віртуальних серверів ІКС, повинні використовуватись криптоалгоритми та криптопротоколи, які визначені національними стандартами, зокрема наведені у переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, визначеному Адміністрацією Держспецзв'язку, та/або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв'язку видано позитивний експертний висновок. Ключі шифрування повинні бути доступні виключно замовнику, адміністратору або технічному адміністратору державних інформаційних ресурсів відповідно до законодавства України у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Засіб КЗІ може бути представлений у вигляді окремого (окремих) засобів або може бути інтегрований до підсистеми віртуалізації ІКС «ЄІССС».

7. Модернізація КСЗІ в ІКС

7.1 Мета модернізації КСЗІ

Мета модернізації КСЗІ – забезпечення захисту інформації, що зберігається, передається та накопичується в ЄІССС та досягнення максимальної ефективності захисту інформації за рахунок одночасного цільового використання усіх необхідних ресурсів, методів і засобів, що виключатимуть несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації: Закон України «Про захист інформації в інформаційно-комунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

КСЗІ ІКС «ЄІССС» повинна передбачати:

– розробку та впровадження комплексу організаційних заходів забезпечення безпеки;

– впровадження апаратно-програмних засобів захисту від НСД;

– забезпечення конфіденційності, цілісності та достовірності інформації при її обробці в ІКС «ЄІССС»;

– забезпечення спостереженості КСЗІ у процесі її функціонування.

Захист інформації має здійснюватися шляхом протидії загрозам, які можна очікувати внаслідок дій порушника на всіх технологічних етапах її обробки і в усіх режимах функціонування ІКС «ЄІССС».

При розробці та впровадженні КСЗІ повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного захисту інформації.

7.2 Призначення КСЗІ в ІКС

КСЗІ в ІКС являє собою сукупність необхідних організаційних та технічних заходів, засобів і методів технічного захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікацій.

КСЗІ в ІКС «ЄІССС» призначена для:

– реалізації політики безпеки інформації, заданої в ІКС «ЄІССС»;

– ідентифікації та автентифікації користувачів у ході надання їм доступу до функцій ІКС «ЄІССС»;

– реалізації функцій криптографічного захисту інформації (КЗІ), що передається каналами зв'язку між компонентами (модулями) ІКС «ЄІССС»;

– забезпечення цілісності та доступності відкритої інформації, що обробляється у ІКС «ЄІССС», а також конфіденційності та цілісності конфіденційної інформації (персональних даних) та технологічної інформації КЗЗ ІКС «ЄІССС»;

– розмежування доступу користувачів до ресурсів;

– створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного сповіщення адміністратора безпеки про факти несанкціонованого доступу до інформації;

– ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи ІКС «ЄІССС», причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;

– керування засобами захисту інформації, контролю за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації ІКС «ЄІССС»;

– 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 ІКС «ЄІССС»;

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

– забезпечення доступності ресурсів ІКС «ЄІССС» для її користувачів;

– забезпечення працездатності та оперативного відновлення ІКС при виникненні позаштатних чи аварійних ситуацій;

– забезпечення захисту обчислювальних ресурсів та компонентів ІКС «ЄІССС» від атак та несанкціонованого доступу з боку мережі Інтернет (в тому числі унеможливлення попадання шкідливого ПЗ до ІКС);

– забезпечення захисту інформації від внесення в програмні компоненти ІКС «ЄІССС» шкідливого програмного коду (вірусів, троянських програм та ін.);

– захист від мережевих атак (кібератак), в тому числі від DOS/DDOS-атак, спроб блокування функціонування ІКС «ЄІССС»;

– захисту інформації, яка обробляється в ІКС «ЄІССС», при її передачі через незахищене середовище (мережа Інтернет);

– забезпечення безпечного підключення до ІКС «ЄІССС» зі сторони зовнішніх ІКС;

– надання права користувачам ІКС «ЄІССС» на виконання відповідних дій, відповідно до їх функцій;

– блокування несанкціонованих дій з інформацією, що потребує захисту, та іншими ресурсами ІКС, локалізації цих дій та ліквідації їх наслідків;

– забезпечення доступності інформації та функцій ІКС «ЄІССС» для її користувачів, а також відмовостійкості компонентів ІКС;

– забезпечення спостереженості за діями користувачів та персоналу ІКС «ЄІССС», реєстрації, збору, зберігання, обробки даних про події, які мають відношення до безпеки інформації, сповіщення адміністратора безпеки про такі події;

– підтримання цілісності критичних ресурсів системи захисту, середовища виконання прикладних програм та інформації в системі, що потребує захисту;

– забезпечення цілісності ПЗ, яке використовується для захисту інформації;

– реєстрація подій, пов'язаних з доступом до інформації та діями щодо неї, результатів ідентифікації в ІКС «ЄІССС», фактів зміни повноважень суб'єктів доступу, тощо;

– забезпечення управління засобами КСЗІ та контролю за її функціонуванням.

Захист від НСД до інформації, яка обробляється в системі, повинен здійснюватися шляхом застосування програмних та апаратно-програмних засобів ТЗІ, функцій захисту програмних та апаратно-програмних засобів, що використовуються в складі ІКС «ЄІССС», впровадженням організаційних та інженерно-технічних заходів.

7.3 Цілі модернізації КСЗІ в ІКС

Цілі модернізації КСЗІ:

– забезпечити максимальний рівень ефективного захисту службової інформації та державних інформаційних ресурсів в ІКС «ЄІССС»;

– забезпечити недопущення блокування інформації, несанкціонованого доступу до неї та/або її модифікації в ІКС за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів;

– досягнення максимальної ефективності захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно- правових актів України у сфері захисту інформації.

8. Вимоги до законодавства України

Модернізація КСЗІ повинно здійснюватися відповідно до вимог нормативно-правових актів у сфері захисту інформації та національних стандартів України з технічного захисту інформації та чинних нормативних документів в галузі технічного захисту інформації (НД ТЗІ), а саме:

Закони України:

– Закон України «Про інформацію» № 2657-XII від 02.10.1992;

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994;

– Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003;

– Закон України «Про наукову і науково-технічну експертизу» № 848-VIII від 26.11.2015;

– Закон України «Про електронні довірчі послуги» від 05 жовтня 2017 року № 2155-VIII;

– Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII;

– Закон України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI;

– Закон України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX.

Укази Президента України:

– Указ Президента України від 27 вересня 1999 року № 1229/99 «Про Положення про технічний захист інформації в Україні»;

– Указ Президента України від 22 травня 1998 року № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні»;

– Указ Президента України від 10 липня 2017 року № 254/2017 «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

Постанови Кабінету Міністрів України:

– Постанова Кабінету Міністрів України від 07 листопада 2018 року № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;

– Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;

– Постанова Кабінету Міністрів України від 09 жовтня 2020 року № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури»;

– Постанова Кабінету Міністрів України від 09 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури»;

– Постанова Кабінету Міністрів України від 23 грудня 2020 року № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»;

– Постанова кабінету Міністрів України від 12 серпня 2009 року № 869 «Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів»;

– Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»;

– Постанова Кабінету Міністрів України від 19 вересня 2018 року № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;

– Постанова Кабінету Міністрів України від 16.11.2002 року № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»;

– Постанова Кабінету Міністрів України від 10.05.2018 року № 357 «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів»;

– Постанова Кабінету Міністрів України від 08.09.2016 року № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів»;

– Постанова Кабінету Міністрів України від 08 лютого 2021 року № 92 «Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

– Постанова Кабінету Міністрів України від 30 грудня 2022 року № 1500 «Деякі питання забезпечення функціонування державних інформаційних ресурсів»

– Постанова Кабінету Міністрів України від 14 квітня 2021 року № 404 «Про затвердження Положення про Єдину інформаційну систему соціальної сфери»;

– Постанова Кабінету Міністрів України від 11.11.2020 № 1278 «Про запровадження експериментального проєкту з реалізації функціоналів першої черги Єдиної інформаційної системи соціальної сфери»;

– Стратегія цифрової трансформації соціальної сфери, схваленої розпорядженням Кабінету Міністрів України від 28.10.2020 № 1353-р.

Нормативні документи системи технічного захисту інформації:

– НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28 квітня 1999 року № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806;

– НД ТЗІ 2.6-001-2011 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах», затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65, із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 № 806;

– НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 24.07.2009 № 172, із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 № 806;

– НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 24.07.2009 № 172.

Накази Держспецзв'язку:

– Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 93 (зі змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку № 567 від 10.10.2012, № 407 від 30.06.2016, № 565 від 13.10.2017, № 483 від 19.08.2020), зареєстрованого в Міністерстві юстиції України 16 липня 2007 року за № 820/14087;

– Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 26 березня 2007 року № 45, зареєстровано в Міністерстві юстиції України 07 липня 2008 року за № 603/15294.

– Вимоги до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, затверджені наказом адміністрації Державної служби спеціального зв'язку та захисту інформації України від 07 травня 2021 року № 278 та зареєстровані в Міністерстві юстиції України 26 травня 2021 року за № 696/36318 (далі – Наказ № 278);

– наказ Адміністрації Держспецзв'язку від 6 жовтня 2021 року № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури».

Державні стандарти:

– ДСТУ 2851-94 «Програмні засоби ЕОМ. Документування результатів робіт», затверджено і введено в дію наказом Держстандарту України від 23.11.1994 № 290;

– ДСТУ 2853-94 «Програмні засоби ЕОМ. Підготовлення і проведення робіт», затверджено і введено в дію наказом Держстандарту України від 23.11.1994 № 290;

– ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів;

– ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;

– ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013, Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки;

– ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;

– ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки;

– ДСТУ ISO/IEC 27018:2019 (ISO/IEC 27018:2019, IDT) Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII.

– ДСТУ ISO/IEC TS 27034-5-1:2019 (ISO/IEC TS 27034-5-1:2018, IDT) Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних керування протоколами та захистом застосунків. Схеми XML.

9. Підготовка загальних вимог до КСЗІ

Інформаційна інфраструктура ІКС «ЄІССС» є різноманітною та розгалуженою, що пов’язано з такими основними чинниками:

– різноманітність інформації за видом та правовим режимом доступу, яка циркулює в ІКС;

– існування великої кількості зовнішніх джерел інформації (державних інформаційних ресурсів) та користувачів.

При наявності зазначених чинників, технологія обробки інформації, вид носіїв інформації є однотипними в ІКС «ЄІССС».

Такий підхід має на меті забезпечити:

– реалізацію відкритої архітектури безпеки, зміст концепції якої надано в ISO 7498-2-89 Information proceeding systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture;

– уніфікацію і оптимізацію матеріальних витрат на проєктування КСЗІ, ця процедура зводиться до проєктування певної кількості типових компонентів, кожен з яких має тільки свої власні дані (для формування бази даних захисту), а не механізми захисту;

– можливість оцінювання кожної складової частини КСЗІ окремо (для будь-якого виду випробувань).

Під КСЗІ в ІКС слід розуміти – взаємопов’язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації ІКС.

З появою нових вимог стосовно захисту інформації, закріплених в нормативно-правових актах України, КСЗІ коригується відповідно до цих вимог.

До складу КСЗІ ІКС «ЄІССС» повинні входити апаратні та програмні засоби захисту від НСД, а також організаційні заходи, спрямовані на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями.

КСЗІ має пройти державну експертизу відповідно до чинного законодавства України, в рамках якої дозволяється, зокрема, провести експертизу засобів ТЗІ і КЗІ в разі відсутності відповідних експертних висновків.

КСЗІ повинна забезпечувати:

– реалізацію заданої політики безпеки інформації;

– забезпечення розмежування доступу користувачів ІКС «ЄІССС» до функцій ІКС та об’єктів, що містять інформацію, яка підлягає захисту, відповідно до прийнятої політики безпеки;

– забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в ІКС «ЄІССС»;

– забезпечення реєстрації дій користувачів ІКС «ЄІССС» по відношенню до функцій ІКС та об’єктів, що містять інформацію, яка підлягає захисту;

– забезпечення захисту інформації від внесення в склад ІКС «ЄІССС» шкідливого програмного коду (вірусів, троянських програм та ін.);

– захист від мережевих атак;

– захисту інформації, яка обробляється в ІКС «ЄІССС», при її передачі через незахищене середовище;

– блокування несанкціонованих дій з інформацією, що потребує захисту, та іншими ресурсами ІКС, локалізації цих дій та ліквідації їх наслідків;

– забезпечення доступності інформації та функцій ІКС «ЄІССС» для її користувачів, а також відмовостійкості компонентів ІКС;

– забезпечення спостереженості за діями користувачів та персоналу, реєстрації, збору, зберігання, обробки даних про події, які мають відношення до безпеки інформації, сповіщення адміністратора безпеки про такі події;

– підтримання цілісності критичних ресурсів системи захисту, середовища виконання прикладних програм та інформації в ІКС «ЄІССС», що потребує захисту;

– підтримку визначеного в політиці безпеки рівня конфіденційності, цілісності, доступності та спостереженості інформації, що обробляється в ІКС «ЄІССС», та технологічної інформації, що забезпечує функціонування компонентів ІКС;

– захист від НСД засобів управління компонентами ІКС «ЄІССС»;

– ідентифікацію користувачів ІКС «ЄІССС»;

– розмежування доступу до ресурсів та процесів ІКС;

– забезпечення управління засобами КСЗІ та контролю за її функціонуванням.

Виконання завдань на РС в ІКС «ЄІССС» повинне забезпечуватись у функціонально замкненому середовищі, в межах якого доступ забезпечується лише до ресурсів, що є необхідними для виконання поставлених перед користувачами завдань, та в межах правил розмежування доступу.

Робота компонентів ІКС «ЄІССС» повинна бути можливою лише за умов функціонування відповідних елементів системи захисту.

Вимоги до надійності функціонування КСЗІ в кожному з режимів роботи повинні бути не нижчими вимог ІКС «ЄІССС» в цілому.

Підготовка загальних вимог до КСЗІ повинна базуватись на виконанні таких завдань:

– обґрунтування необхідності модернізації КСЗІ, аналіз і визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

– обстеження середовища функціонування КСЗІ з аналізом та описом системи, інформаційного та фізичного середовища, а також середовища користувачів з метою підготовки вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС «ЄІССС» та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах послуг;

– затвердження переліку об’єктів захисту;

– визначення потенційних загроз для інформації;

– розробка моделі загроз;

– формування технічного завдання на модернізацію КСЗІ має здійснюватися із урахуванням результатів аналізу, обстеження, та вимоги обов'язкового використання наявних в ДПС КЗЗ;

– визначення ризиків і переліку суттєвих загроз;

– розробка технічного завдання на модернізацію КСЗІ.

9.1 Розробка та оформлення політики безпеки інформації в КСЗІ, здійснення вибору основних рішень з протидії всім суттєвим загрозам

Політики безпеки розробляються згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБУ від 22.04.1999 № 22 та рекомендаціями НД ТЗІ 1.4-001-00 «Типове положення про службу захисту інформації в автоматизованій системі», затверджений наказом ДСТСЗІ СБУ від 04.12.2000 № 53.

В ІКС необхідно затвердити політику інформаційної безпеки, яка визначає:

– мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо в ІКС;

– опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів ІКС, які задіяні в цьому процесі;

– вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об'єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами. При цьому необхідно дотримуватися принципу надання необхідних та мінімально достатніх повноважень користувачам та адміністраторам відповідно до їх службових обов'язків;

– політику фізичної безпеки та захисту ІКС від навколишнього природного середовища;

– вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

– політику управління обліковими записами в програмному та апаратному забезпеченні ІКС. Політика повинна визначати порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах ІКС;

– вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів ІКС. Повинні бути визначені також вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача за певної кількості спроб підбору пароля, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

– політику забезпечення безперебійної роботи ІКС, зокрема порядок резервування даних та компонентів ІКС, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів ІКС у випадку виходу їх з ладу тощо;

– порядок дій персоналу ІКС у випадках відмов або збоїв ІКС в цілому або окремих його компонентів;

– порядок використання змінних (зовнішніх) пристроїв та носіїв інформації в ІКС (за наявності);

– політику мережевого захисту, зокрема щодо сегментації мережі ІКС, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

– політику проведення модернізації (оновлення) компонентів ІКС, внесення змін до складу та в налаштування компонентів ІКС. Повинні бути визначені відповідальні особи, які мають право проводити ці робити, а також порядок дотримання політики безпеки, яка прийнята в ІКС, під час проведення таких робіт;

– опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів ІКС, які задіяні в цьому процесі;

– політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об’єкта);

– політику реєстрації та аудиту подій, що реєструються компонентами ІКС. Політика повинна містити перелік подій, які реєструються кожним компонентом ІКС, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами ІКС на предмет виявлення ознак кібератак або кіберінцидентів;

– політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб об’єкта критичної інфраструктури, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп’ютерні надзвичайні події);

– політику використання веб-інтерфейсів користувачами ІКС;

– політику проведення внутрішнього аудиту інформаційної безпеки ІКС.

Повинен бути встановлений порядок внесення змін до таких документів.

Вимоги затвердженої в ІКС політики інформаційної безпеки повинні бути доведені під підпис або в інший спосіб до всіх його працівників. В ІКС повинна бути визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки.

9.2 Розробка модернізованого технічного завдання на модернізацію КСЗІ

Розробка технічного завдання на модернізацію КСЗІ має забезпечувати наступне:

– визначення завдання захисту інформації в ІКС «ЄІССС», мета модернізації КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту;

– здійснення аналізу ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначення переліку суттєвих загроз;

– визначення загальних структур та складів КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимих обмежень щодо застосування певних заходів і засобів, інших обмежень щодо середовищ функціонування ІКС «ЄІССС», обмежень щодо використання ресурсів ІКС для реалізації задач захисту, припустимих витрат на модернізацію КСЗІ, умов створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальних вимог до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що увійдуть до складу КСЗІ;

– визначення об’єктів захисту, суб’єктів доступу, процесів, правил розмежування доступу;

– обов’язкове використання засобів КЗЗ з підтвердженою відповідністю;

З метою забезпечення конфіденційності та цілісності об’єктів захисту ІКС «ЄІССС», які передаються через незахищене середовище необхідно використовувати криптографічні засоби захисту (далі – засіб КЗІ), які мають чинний, позитивний експертний висновок Адміністрації Держспецзв'язку в сфері КЗІ, та, відповідно до нього можуть здійснювати захист конфіденційної інформації у каналах зв’язку. Засіб КЗІ може бути представлений у вигляді окремого (окремих) засобів або може бути інтегрований до ПЗ ІКС «ЄІССС».

9.3 Розробка модернізованого проєкту КСЗІ

1. Розробку техноробочого проєкту КСЗІ з відповідним пакетом документації:

– Пояснювальна записка

– Опис програмних засобів

– Опис технічних засобів.

2. Розробку організаційно-розпорядчої документації КСЗІ:

– проєкт акту категоріювання;

– проєкт наказу про призначення комісії з категоріювання та обстеження;

– проєкт наказу про призначення комісії для проведення попередніх випробувань КСЗІ в ІКС;

– проєкт наказу про створення комісії для приймання КСЗІ в дослідну експлуатацію;

– проєкти актів про приймання у дослідну експлуатацію КСЗІ в ІКС;

– проєкти актів про завершення дослідної експлуатації КСЗІ в ІКС;

– розробку документації щодо проведених випробувань КСЗІ:

– програми та методики випробувань КСЗІ в ІКС;

– протоколи попередніх випробувань КСЗІ в ІКС.

3. Розробку експлуатаційної документації КСЗІ:

До складу експлуатаційної документації мають входити технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ (згідно НД ТЗІ 2.6-001-2011), які містять інструкції щодо організації антивірусного захисту в ІКС, щодо правил налаштування параметрів безпеки компонентів КЗЗ ІКС (допускається використовувати експлуатаційну документацію на КЗЗ), щодо правил експлуатації, модернізації та проведення ремонтних робіт в ІКС.

Експлуатаційна документація може бути викладена, як у вигляді окремих настанов (інструкцій), так і поєднуватись за тематикою у єдиний документ.

Технологічні (операційні) інструкції (настанови) щодо виконання завдань з адміністрування та обслуговування КСЗІ (згідно НД ТЗІ 2.6-001-2011) підлягають в рамках розробки експлуатаційної документації чи відокремленої робочої.

4. Формуляр;

5. Реєстраційні журнали, використовувані для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

9.4 Введення КСЗІ в дію та оцінка захищеності інформації в ІКС

Введення КСЗІ в дію та оцінка захищеності інформації в ІКС «ЄІССС» повинні відповідати таким завданням та задовольняти наступним вимогам:

– проведення робіт з підготовки організаційних структур та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС;

– проведення попередніх випробувань згідно з програмами та методиками випробувань, перевірка працездатності КСЗІ та визначення можливості прийняття їх у дослідну експлуатацію, оформлення протоколів випробувань;

– проведення дослідної експлуатації, під час якої відпрацьовуються технології обробки інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів.

9.5 Організація, координація та супроводження державної експертизи

Супроводження проведення додаткової державної експертизи повинне забезпечувати виконання наступних завдань:

– супроводження проведення додаткової державної експертизи КСЗІ з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію;

– усунення недоліків у разі їх виявлення під час проведення державної експертизи.

10. СКЛАД ТА ЗМІСТ ПОСЛУГ ІЗ МОДЕРНІЗАЦІЇ КСЗІ в ІКС

Склад та зміст послуг з розробки КСЗІ в ІКС «ЄІССС» передбачає наступні етапи:

1-й етап

Обстеження середовищ функціонування ІКС «ЄІССС» та розробка ТЗ на модернізацію КСЗІ в ІКС «ЄІССС». Узгодження ТЗ з ДССЗЗІ України:

Підготовка організаційно-розпорядчої документації.

Фахівці Виконавця проводять аналіз організаційно-розпорядчих документів Замовника і нормативно-правових документів в області захисту інформації, що впливають на діяльність Замовника.

За результатами проведеного аналізу Виконавець, спираючись на нормативну базу, що діє в Україні у сфері захисту інформації, готує проєкти документів, які визначають організаційну складову КСЗІ (проєкт акту категоріювання, проєкт наказу про призначення комісії з категоріювання та обстеження, проєкт наказу про призначення комісії для проведення попередніх випробувань КСЗІ в ІКС, проєкти посадових інструкцій і процедур та ін.), які затверджуються Замовником.

Обстеження інформаційної інфраструктури Замовника.

Виконавець проводить обстеження ІКС Замовника. Аналізується архітектура системи, її топологія і складові елементи. Визначаються типи користувачів системи, типізується інформація, що обробляється в ІКС.

Результати обстеження середовищ функціонування ІКС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІКС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001-2000.

За результатами обстеження середовищ функціонування ІКС затверджується перелік об’єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001-2000, НД ТЗІ 2.5-008-2002, НД ТЗІ 2.5-010-2003 щодо класифікації об’єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000.

Розробка пакету документів «План захисту інформації».

План захисту інформації розробляється в рамках документації, що розробляється на етапі виконання передпроектних робіт. (НД ТЗІ 2.6-001-11).

Виконавець розробляє наступний пакет документів, який затверджується Замовником:

– Перелік інформації, що підлягає автоматизованому обробленню в ІКС;

– Модель порушника безпеки інформації;

– Модель загроз для інформації;

– Політика безпеки;

– План захисту інформації.

У переліку інформації, що підлягає автоматизованому обробленню в ІКС та потребує захисту, має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІКС, класифікований за такими ознаками:

– семантичний вміст відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;

– характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (ІДТ, КІВД, КІ, ВІВД, ВІ);

– вищий ступінь обмеження доступу (для ІДТ) до інформації (ступінь секретності) відповідно до вимог Зводу відомостей, що становлять державну таємницю;

– критичні властивості інформації з погляду забезпечення її захищеності, визначені з урахуванням вимог Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах і вимог власника (розпорядника) інформації;

– вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІКС різних категорій.

Виконавець використовуючи результати обстеження ІКС здійснює аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначає перелік суттєвих загроз. Результати аналізу ризиків оформлюються в Моделі порушника безпеки інформації, Моделі загроз для інформації згідно з НД ТЗІ 2.6-001-11.

Опис політики безпеки інформації в ІКС повинен містити набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок оброблення в ІКС інформації, зазначеної у Переліку інформації, що підлягає автоматизованому обробленню в ІКС та потребує захисту, та спрямовані на захист її критичних властивостей від загроз, притаманних умовам функціонування конкретної ІКС. Відповідно до рекомендацій НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000 в Описі політики безпеки інформації в ІКС повинні бути (з урахуванням результатів обстеження середовищ функціонування ІКС) визначені інформаційні ресурси ІКС, що потребують захисту. Мають бути сформульовані основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу та вимоги щодо захисту від цих загроз. Як складові частини загальної політики безпеки інформації в ІКС повинні бути наведені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політика забезпечення спостереженості ІКС.

План захисту інформації має визначати загальну структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту інші обмеження щодо середовищ функціонування ІКС, обмеження щодо використання ресурсів ІКС для реалізації задач захисту, припустимі витрати на модернізацію КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІКС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Розробка технічного завдання на модернізацію КСЗІ.

Фахівці Виконавця розробляють і погоджують із Замовником документ «Технічне завдання на модернізацію КСЗІ», яке визначає всі основні вимоги до КСЗІ і можливі варіанти реалізації її складових елементів. Після затвердження технічного завдання на модернізацію КСЗІ Замовником, документ узгоджується з ДССЗЗІ України.

2й етап

Модернізація КСЗІ в ІКС «ЄІССС»

Розробка техноробочого проєкту на модернізацію КСЗІ.

Після узгодження технічного завдання на модернізацію з контролюючим органом Виконавець розробляє пакет документів техноробочого проєкту на модернізацію. Техноробочий проєкт на модернізацію є комплектом документів, в який входить частина документів, розроблених на попередніх етапах і ряд нових документів, в яких описано, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься КСЗІ.

Техноробочий проєкт на модернізацію розробляється на підставі і відповідно до технічного завдання на модернізацію. Під час розробки проєкту КСЗІ обґрунтовуються і приймаються проєктні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

В результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

На даному етапі має бути розроблений наступний пакет документів:

– техноробочий проєкт;

– інструкції з експлуатації КСЗІ та її елементів;

– процедури регламентного обслуговування КСЗІ;

– правила і положення по проведенню тестування і аналізу роботи КСЗІ;

– керівництва адміністраторів і користувачів;

– формуляр КСЗІ ІКС.

Вимоги до документації та методичного забезпечення щодо першого та другого етапів можуть бути уточнені в Технічному завданні.

3й етап

Впровадження КСЗІ в ІКС «ЄІССС»

Приведення інформаційної інфраструктури Замовника у відповідність до техноробочого проєкту на модернізацію.

Проводиться надання послуг з приведення інформаційної інфраструктури замовника у відповідність до техноробочого проєкту на модернізацію.

Проведення пусконалагоджувальних робіт та навчання користувачів.

Виконавець проводить всі пусконалагоджувальні роботи, навчання та інструктажі персоналу Замовника згідно з правилами і режимами експлуатації КСЗІ.

Проводяться наступні заходи:

– організація захисту інформації від несанкціонованого доступу (НСД);

– організація антивірусного захисту інформації;

– розробка програми і методики попередніх випробувань;

– проведення попередніх випробувань.

Випробування КСЗІ.

Проводяться попередні випробування КСЗІ з метою підтвердження результативності її роботи і відповідності положенням, визначеним у технічному завданні на модернізацію.

У процесі випробувань виконуються тестові завдання і контролюються отримані результати, які і є індикатором працездатності спроєктованої КСЗІ.

За результатами попередніх випробувань оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

Проводиться дослідна експлуатація, під час якої:

– відпрацьовуються технології обробки інформації, обліку машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів ІКС і автоматизованого контролю за діями користувачів;

– співробітники служби захисту інформації і користувачі ІКС набувають практичних навичок з використання технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядчих документів з питань розмежування доступу до технічних засобів і інформаційних ресурсів;

– здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагодження та конфігурування КЗЗ;

– здійснюється (за необхідністю) коригування робочої та експлуатаційної документації;

– виконавець надає, в паперовому вигляді та на електронному носії, проєктну, технічну та експлуатаційну документацію.

За результатами дослідної експлуатації приймається рішення щодо готовності КСЗІ в ІКС до подання на державну експертизу.

4й етап

Організація, координація та супроводження державної експертизи

Етап проведення державної експертизи КСЗІ і отримання Атестата відповідності складається з:

– підготовки КСЗІ до проведення державної експертизи в ДССЗЗІ і супроводу експертних випробувань;

– узгодження з ДССЗЗІ результатів експертизи і видача Замовникові Атестата відповідності.

Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню на модернізацію, вимогам нормативної документації щодо захисту інформації і визначення можливості введення КСЗІ на ІКС в експлуатацію.

11. Опис Послуги

Таблиця 10.1 – Опис послуг модернізації КСЗІ в ІКС

№ з/п	Назва етапу	Сутність етапц	Результати проведення етапу
1.	Попереднє ознайомлення та обстеження ІКС «ЄІССС»	Проведення аналізу організаційно-розпорядчих документів ПФУ та Мінсоцполітики: організаційна структура, штатний розклад, положення про відділи й посадові інструкції співробітників, пов'язаних з експлуатацією ІКС «ЄІССС», документи, що регламентують доступ до ІКС «ЄІССС» тощо. Проведення аналізу нормативно-правових документів в сфері захисту інформації, до яких належать Закони України, постанови Кабінету Міністрів України, накази Державної служби спеціального зв'язку й захисту інформації України (далі – Держспецзв'язку), що встановлюють правила роботи з інформацією. Підготовка проєктів документів, які визначають організаційну складову КСЗІ, які затверджуються Мінсоцполітики та узгоджуються з ПФУ. Проведення обстеження ІКС «ЄІССС» та її складових. Аналізується архітектура системи, її топологія й складові елементи. Визначення типи користувачів системи, типізується інформація, оброблювана в ІКС. За результатами готується наступні, зокрема проєкти документів: Акт обстеження середовищ функціонування ІКС, зокрема, який повинен містити опис, принципи побудови й архітектуру ІКС (НД ТЗІ 3.7-003-05), перелік об'єктів ІКС, що потребують захисту (НД ТЗІ 3.7-003-05) які затверджуються Мінсоцполітики та узгоджуються з ПФУ. Розробка Плану захисту інформації: Політика безпеки ІКС «ЄІССС» (Політика захисту інформації) (НД ТЗІ 1.4-001-00, НД ТЗІ 3.7-003-05) Модель загроз інформації та модель порушника безпеки інформації ІКС «ЄІССС» (НД ТЗІ 3.7-003-05), які затверджуються Мінсоцполітики та узгоджуються з ПФУ.	- Проєкт акту обстеження середовищ функціонування модифікованої ІКС «ЄІССС». - Документація передпроєктних робіт КСЗІ в ІКС «ЄІССС» (Перелік інформації, що підлягає автоматизованому обробленню в ІКС, Модель порушника безпеки інформації, Модель загроз для інформації, Політика безпеки, План захисту)
2.	Розробка технічного завдання на КСЗІ в ІКС «ЄІССС»	Розробка, погодження Технічного завдання на модернізацію КСЗІ ІКС «ЄІССС» (НД ТЗІ 3.7-001-99, НД ТЗІ 3.7-003-05), що визначає всі основні вимоги до КСЗІ й можливі шляхи реалізації її складових елементів. Узгодження Технічного завдання на модернізацію з Держспецзв'язку.	Модернізоване Технічне завдання на КСЗІ в ІКС «ЄІССС»

№ з/п	Назва етапу	Сутність етапц	Результати проведення етапу
3.	Розробка проєктної та експлуатаційної документації на КСЗІ в ІКС «ЄІССС»	Проектування КСЗІ та розробка проєктної документації (НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-05): Техноробочий проєкт КСЗІ. Приведення інформаційної інфраструктури у відповідність із техноробочими проєктом на модернізацію. Розробка Експлуатаційної документації на КСЗІ, що включає: інструкції експлуатації КСЗІ і її елементів; процедури регламентного обслуговування КСЗІ; правила й положення по проведенню тестування й аналізу роботи КСЗІ.	1. Документація техноробочого проєкту КСЗІ в ІКС «ЄІССС» (Пояснювальна записка; Опис комплексу технічних засобів; Опис програмного забезпечення). 2. Робоча документація на КСЗІ в ІКС «ЄІССС» (інструкція з організації парольного захисту в ІКС «ЄІССС»; інструкція адміністратора системи ІКС «ЄІССС» в частині забезпечення захисту інформації; інструкція адміністратора безпеки ІКС «ЄІССС» в частині забезпечення захисту інформації; інструкція користувача ІКС «ЄІССС» в частині забезпечення захисту інформації; інструкції іншого адміністративного персоналу (*за необхідності*). 3. Експлуатаційна документація КСЗІ в ІКС «ЄІССС» (інструкція про порядок модернізації КСЗІ в ІКС «ЄІССС» ; інструкція про порядок резервування та відновлення інформації в ІКС «ЄІССС»; інструкція про організацію контролю за функціонуванням КСЗІ в ІКС «ЄІССС»; інструкція про порядок забезпечення антивірусного захисту ІКС «ЄІССС»).
4.	Розробка програми та методики попередніх випробувань КСЗІ в ІКС «ЄІССС»	Розробка Програми та методик випробувань КСЗІ в ІКС «ЄІССС» (НД ТЗІ 3.7-003-05).	Програма та методика попередніх випробувань КСЗІ в ІКС «ЄІССС»
5.	Проведення попередніх випробувань КСЗІ в ІКС «ЄІССС»	Проведення попередніх випробувань КСЗІ, з метою підтвердження результативності її роботи й відповідності положенням, визначеним в Технічному завданні на модернізовану КСЗІ. Підготовка Протоколу(ів) попередніх випробувань КСЗІ в ІКС «ЄІССС» (НД ТЗІ 3.7-003-05).	Протокол попередніх випробувань КСЗІ в ІКС «ЄІССС»
6.	Дослідна експлуатація КСЗІ	Проведення дослідної експлуатації, доопрацювання складових частин КСЗІ та корегування робочої документації за результатами дослідної експлуатації. Акт про приймання КСЗІ в дослідну експлуатацію (НД ТЗІ 3.7-003-05). Підготовка висновку щодо можливості подання КСЗІ на державну експертизу.	Проєкти документів: - акту приймання КСЗІ ІКС «ЄІССС» у дослідну експлуатацію; - акту завершення дослідної експлуатації КСЗІ в ІКС «ЄІССС»

№ з/п	Назва етапу	Сутність етапц	Результати проведення етапу
7.	Організація проведення додаткової державної експертизи КСЗІ	Підготовка проєкту Заявки на проведення державної експертизи КСЗІ в ІКС «ЄІССС» та визначення організатора експертизи КСЗІ в ІКС «ЄІССС». Супроводження державної експертизи КСЗІ в ІКС «ЄІССС» відповідно вимог Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 93 та НД ТЗІ 2.6-001-2011. Під час проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС» Організатором експертизи розробляється та надається: Програма проведення додаткової державної експертизи КСЗІ а ІКС «ЄІССС». (НД ТЗІ 3.7-003-05), Методика проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС» (НД ТЗІ 3.7-003-05, не надається Замовнику відповідно до Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 93). Організатором експертизи здійснюється: - проведення досліджень та експертного оцінювання КСЗІ в ІКС «ЄІССС» відповідно до методик проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС»; - оформлення результатів експертизи та підготовка протоколу експертних випробувань, експертного висновку та атестату відповідності КСЗІ в ІКС «ЄІССС»; -одержання Експертного висновку та Атестату відповідності КСЗІ в ІКС «ЄІССС» за результатами проведення експертизи КСЗІ ІКС.	1. Проєкт Заявки на проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС» та визначення Організатора експертизи. 2. Програма проведення додаткової державної експертизи КСЗІ а ІКС «ЄІССС». 3. Методика проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС». (не надається Замовнику відповідно до Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 93) 4. Протокол виконання експертних робіт відповідно до методик проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС». 5. Експертний висновок та Атестат відповідності за результатами проведення додаткової державної експертизи КСЗІ в ІКС «ЄІССС».

Відповідно до НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» ІКС «ЄІССС» відноситься до автоматизованої системи класу 3. Найвищий гриф оброблюваної інформації – конфіденційна (персональні дані, державні інформаційні ресурси) та технологічна інформація (таблиці даних тощо).

Допускається виконувати окремі етапи послуг до завершення попередніх етапів, паралельно у часі виконання етапів послуг.

12. Порядок контролю та приймання послуг

Контроль та прийом наданих послуг здійснюється на території Замовника.

По закінченні послуг (етапу послуг) Виконавець надає Замовнику акт приймання–передачі наданих Послуг в паперовому вигляді, а також документацію, яка передбачена умовами договору згідно з Календарним планом та технічних вимог, в електронному вигляді на магнітному носієві інформації (у вигляді цифрових файлів) – 1 прим. та в паперовому вигляді – 1 прим.