ПОГОДЖУЮ
Голова Державного агентства з питань електронного урядування України
_____О.В. Риженко

«___» _____ 2018 р.

ЗАТВЕРДЖУЮ
Президент міжнародної благодійної організації «Фонд Східна Європа»
_____ В.В. Лях

«___» _____ 2018 р.

ТЕХНІЧНІ ВИМОГИ

На виконання робіт зі створення комплексної системи захисту інформації Єдиного державного веб-порталу відкритих даних

Київ 2018

Зміст

1. ЗАГАЛЬНІ ВІДОМОСТІ

Даний документ вміщує основні вимоги щодо технічного оснащення Комплексної системи захисту інформації Єдиного державного веб-порталу відкритих даних Державного агентства з питань електронного урядування України, під час якого повинна бути проведена робота з налаштування комплексу засобів захисту, що входять до складу Єдиного державного веб-порталу відкритих даних в тому числі монтажу та пусконалагоджувальних робіт підсистеми криптографічного захисту, що повинна постачатись в рамках виконуваних робіт.

Виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії згідно із частиною 3 пункту 23 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 26 березня 2006 року № 373.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

Терміни вживаються у значеннях, наведених в нормативно-правових актах та нормативних документах зазначених у даному документі.

Скорочення	**Опис**
Портал	- Єдиний державний веб-портал відкритих даних
АБ	- адміністратор безпеки
БД	- база даних
Держагентство	- Державне агентство з питань електронного урядування України
ДССЗЗІ або Держспецзв'язку	- Державна служба спеціального зв'язку та захисту інформації України
ІзОД	- інформація з обмеженим доступом
ІТС	- інформаційно-телекомунікаційна система
КЗЗ	- комплекс засобів захисту
КЗІ	- криптографічний захист інформації
КСЗІ	- комплексна система захисту інформації
НД	- нормативний документ
НПА	- нормативно-правові акти
НСД	- несанкціонований доступ
ОС	- операційна система
ПЗ	- програмне забезпечення
СКБД	- система керування базами даних
ТВ	- Технічні вимоги
ТЗ	- технічне завдання

3. ОСНОВНА МЕТА ТА ПРИЗАЧЕННЯ ЄДИНОГО ВЕБ-ПОРТАЛУ ВІДКРИТИХ ДАНИХ

Основною метою створення Порталу є забезпечення ефективності використання публічної інформації органів виконавчої влади для підвищення відкритості і прозорості їх діяльності, встановлення вимог до розпорядників інформації щодо надання та оприлюднення інформації у формі відкритих даних.

Портал орієнтовано на задоволення потреб інститутів громадянського суспільства, представників громадськості, науковців, представників засобів масової інформації та інших відвідувачів, які зацікавлені діяльністю органів виконавчої влади.

Цілі створення Порталу:

- забезпечення своєчасного розміщення органами влади інформації, яка підлягає оприлюдненню, а також будь-яких інших даних, що відповідають визначенню публічної інформації у формі відкритих даних;
- оприлюднення та регулярне оновлення розпорядником інформації відкритих даних на його веб-сторінці Порталу;
- забезпечення для всіх користувачів єдиного інформаційного простору, а також встановлення єдиних стандартів розміщення інформаційних матеріалів;
- забезпечення своєчасного розміщення повної та достовірної інформації;
- забезпечення ефективних двосторонніх комунікацій і каналів зворотного зв’язку;
- забезпечення зручної навігації та пошуку по всьому інформаційному наповненні Порталу;
- отримання зворотного зв’язку розпорядниками від користувачів;
- формування бази запитів щодо наборів;
- створення спільноти для обговорення питань щодо відкритих даних на форумі;
- розвиток API порталу щодо завантаження даних розпорядниками та скачування користувачами;
- підтримка харвестінгу на завантаження наборів та їх експорт.

Єдиний державний веб-портал відкритих даних призначений для забезпечення надання доступу до публічної інформації у формі відкритих даних та передбачає доступ до інформації органів виконавчої влади з можливістю її наступного використання в найрізноманітніших цілях: наукові дослідження, інновації, бізнес проекти, підзвітність та суспільний контроль за органами влади тощо.

4. ХАРАКТЕРИСТИКА ЄДИНОГО ВЕБ-ПОРТАЛУ ВІДКРИТИХ ДАНИХ

Єдиний державний веб-портал відкритих даних - комплексна інформаційна система, цільовою функцією якої є забезпечення централізованого зберігання описової та посилальної інформації за відкритими даними органів державної влади, органів місцевого самоврядування та організацій, що діють на території України, а також безпосередньо самих наборів відкритих даних (за потреби).

Комплексність порталу відкритих даних обумовлена необхідністю реалізації не тільки цільової функції, а й інших функцій, що забезпечують реалізацію державної політики України в галузі публікації відкритих даних, у тому числі проведення моніторингу, формування тематичних спільнот в мережі Інтернет, оцінки затребуваності відкритих даних.

4.1. Загальний склад Порталу.

Портал складається з таких функціональних модулів:

- Модуль інформаційної взаємодії з джерелами відкритих даних і зберігання відкритих даних - призначений для централізованого обліку інформації (відкриті дані);
- Модуль класифікації та пошуку - призначений для систематизованої класифікації всіх наборів даних, зібраних на Порталі. Повинен виконувати функції навігації і пошуку по наборах відкритих даних на Порталі;
- Інформаційно-аналітичний модуль – призначений для забезпечення інформаційного представлення і публічного доступу до відкритих державних даними громадянам, державним та іншим організаціям шляхом надання інформації через портал;
- Модуль колективної роботи та обговорення - призначений для обміну думками між зацікавленими користувачами різних тематик області відкритих даних, для можливості загального обговорення та контролю якості відкритих даних;
- Модуль адміністрування - призначений для управління доступом, резервного копіювання і відновлення, діагностування Порталу та управління його конфігураціями.

Для Порталу створено API, що надає можливість профільним органам влади автоматично під’єднуватися до нього і публікувати необхідні набори даних із безпосереднього середовища роботи: веб-сайт, адмін-панель, тощо. API сервіс який включає механізм аутентифікації, та містить всі необхідні атрибути наборів даних у якості параметрів інтерфейсу створення.

Server-side Web API забезпечує можливість повністю автоматизованого (без участі людини) доступу до всієї інформації набору даних шляхом їх перегляду та читання (без можливості внесення змін) за запитом у цілодобовому режимі без вихідних (за основу взятий стандартний інтерфейс прикладного програмування CKAN).

Сервіс API також забезпечує можливість отримання повного переліку наборів даних із метаданими та інтероперабельність із іншими порталами (каталогами) відкритих даних (зокрема забір інформації з використанням модулю CKAN Data Harvester).

4.2. Загальний опис алгоритму роботи та функціонування Порталу.

Розпорядник відкритих даних, який зареєстрований в системі та пройшов успішну аутентифікацію, має можливість завантаження (публікації) відкритих даних в ручному режимі або через API.

Користувач має можливість отримання даних в ручному режимі шляхом візуалізації через відповідні механізми веб-сервера, або в автоматичному режимі через програмні інтерфейси Web API, безпосередньо в додаток користувача. Також, користувач має можливість реєстрації власних додатків, що працюють з відкритими даними, для їх розповсюдження.

4.3. Характеристика інформації що обробляється на Порталі.

Найвищий гриф обмеження доступу до інформації, яка може циркулювати на Порталі та підлягає захисту – відкрита інформація.

Інформація з обмеженим доступом на Порталі не циркулює. У випадку оприлюднення інформації ІзОД власник (розпорядник) інформації персонально несе відповідальність за розголошення таких відомостей у встановленому законодавством порядку.

За рівнем обмеження доступу інформація, яка циркулює на Порталі поділяється на:

1. Відкриту інформацію.
2. Технологічну інформацію.

До **відкритої інформації** відносяться:

- інформаційні ресурси загального користування – інформаційні об’єкти, що містять матеріали інформаційно-довідкового характеру на Порталі, доступні всім користувачам Порталу (інформаційні ресурси загального користування представлені у вигляді – папок, файлів, електронних листів, Веб-сторінок);
- описова та посилальна інформація за відкритими даними органів державної влади, органів місцевого самоврядування та організацій, що діють на території України (спеціальні інформаційні ресурси представлені у вигляді - файлів, записів таблиць БД, Веб-сторінок);
- набори відкритих даних органів державної влади, органів місцевого самоврядування та організацій, що діють на території України, які зберігаються на Порталі (спеціальні інформаційні ресурси представлені у вигляді - папок, файлів, електронних листів, записів таблиць БД, Веб-сторінок).

Ця інформація підлягає захисту в частині збереження цілісності, а для наборів відкритих даних ще й автентичності, та забезпечення її доступності.

До **технологічної інформації** відноситься:

- технологічна інформація КСЗІ та технологічна інформація щодо адміністрування та управління компонентами Порталу;
- дані про персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів захисту, інформація журналів реєстрації дій користувачів, інша інформація КЗЗ, інформація про профілі та настройки обладнання та режими його функціонування, робочі параметри прикладного програмного забезпечення, ключова інформація для криптографічних перетворень тощо.

Технологічна інформація Порталу призначена для використання тільки уповноваженими користувачами з числа адміністраторів Порталу.

Ця інформація підлягає захисту в частині збереження конфіденційності, цілісності та забезпечення її доступності.

5. ПРИЗНАЧЕННЯ КСЗІ ЄДИНОГО ВЕБ-ПОРТАЛУ ВІДКРИТИХ ДАНИХ

КСЗІ Порталу забезпечує захист інформації, що обробляється та зберігається в межах Єдиного веб-порталу відкритих даних від несанкціонованого доступу, порушення цілісності та доступності відкритої інформації, конфіденційності технологічної інформації, а також несанкціонованої модифікації та знищення інформації.

КСЗІ Порталу призначена для:

– формування та реалізації політики безпеки інформації, прийнятої на Порталі;

– захисту складових Порталу та інформації, яка обробляється програмними засобами Порталу від несанкціонованого доступу, модифікації та знищення;

– забезпечення цілісності та доступності інформації, яка циркулює на Порталі;

– забезпечення цілісності, доступності та спостережності інформації, для авторизованих користувачів;

– захисту конфіденційності, цілісності та доступності технологічної інформації щодо функціонування системи, яка повинна бути доступна тільки уповноваженому персоналу, що забезпечує управління програмними та технічними засобами Порталу;

– постійного моніторингу та аудиту подій на Порталі, які мають відношення до безпеки інформації, а також для забезпечення постійного контролю та керування станом захищеності Порталу;

– забезпечення працездатності та оперативного відновлення компонентів Порталу при виникненні нештатних чи аварійних ситуацій.

Захист від несанкціонованого доступу до інформації, яка циркулює в системі, повинен здійснюватися шляхом застосування програмно-апаратних засобів і методів технічного захисту інформації, функцій захисту програмного забезпечення та обладнання, що використовується в складі Порталу, впровадженням організаційних та інженерно-технічних заходів.

Вимоги до захисту Порталу у частині витоку інформації технічними або іншими каналами не висуваються.

Захист Порталу від ймовірних зовнішніх атак забезпечується засобами захисту центру обміну даними Секретаріату Кабінету Міністрів України та захищених вузлів Інтернет доступу відповідних Інтернет провайдерів та не входить до кола завдань цих Технічних вимог.

Враховуючи, що адміністрування Порталу здійснюється віддалено, із використанням відкритих каналів мережі Інтернет, з метою реалізації захисту технологічної інформації, що передається для здійснення адміністрування компонентів Порталу, необхідно впровадити підсистему криптографічного захисту інформації, що забезпечуватиме захист каналів передачі даних.

З метою забезпечення цілісності та автентичності даних, що передаються до Порталу, необхідно впровадити підсистему криптографічного захисту інформації, що забезпечуватиме накладання/перевірку електронного цифрового підпису на інформацію, що передаватиметься до Порталу.

6. ВИМОГИ ЩОДО ПОБУДОВИ КСЗІ ЄДИНОГО ВЕБ-ПОРТАЛУ ВІДКРИТИХ ДАНИХ

В рамках виконання робіт з побудови КСЗІ Єдиного веб-порталу відкритих даних Виконавець повинен виконати наступні роботи:

6.1. Формування загальних вимог до КСЗІ

6.1.1. Обстеження середовищ функціонування Порталу

З метою визначення об'єму побудови КСЗІ і розроблення політики безпеки КСЗІ Порталу необхідно провести обстеження середовищ функціонування Порталу.

Під час проведення первинного обстеження Портал повинен розглядатись як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

У відповідності до НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» під час проведення обстеження середовищ функціонування Порталу необхідно провести:

- Обстеження фізичного середовища Порталу;Обстеження обчислювальної системи Порталу;
- Обстеження інформаційного середовища Порталу;
- Обстеження середовища користувачів Порталу.

За результатами обстеження середовищ функціонування Порталу затверджується перелік об’єктів захисту, а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника.

6.1.2. Формування завдання на створення КСЗІ

На цьому етапі:

- визначаються завдання захисту інформації Порталу, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту;

- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

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

6.2. Розробка політики безпеки інформації на Порталі

На цьому етапі здійснюється:

- вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації на Порталі, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

- документальне оформлення політики безпеки інформації.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Політику безпеки рекомендується оформляти у вигляді окремого документу або розділу Плану захисту.

6.3. Розробка Технічного завдання КСЗІ Порталу.

Технічне завдання на КСЗІ має бути розроблене з урахуванням вимог НД ТЗІ 3.7-001-99. Технічне завдання ґрунтується на результатах обстеження.

Інші послуги надаються відповідно до вимог технічного завдання на створення КСЗІ ІТС, розробленого в рамках цього ж проекту (пункт 4.1.) та погодженого Адміністрацією Держспецзв'язку України у встановленому порядку.

Технічне завдання повинно містити такі основні підрозділи:

- загальні відомості;
- мета і призначення комплексної системи захисту інформації;
- загальна характеристика автоматизованої системи та умов її функціонування;
- вимоги до комплексної системи захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до ТЗ;
- порядок проведення випробувань комплексної системи захисту інформації.

6.4. Розробка проектної та експлуатаційної документації КСЗІ Порталу.

В процесі проектування КСЗІ Порталу Виконавець повинен розробити та погодити з Замовником комплекти технічної та експлуатаційної документації.

Проектна документація на КСЗІ Порталу повинна містити проектні рішення щодо побудови системи та опис її компонентів.

Склад та зміст документації повинен відповідати вимогам ГОСТ 34.201-89, РД 50-34.698-90, НД ТЗІ 3.7-003-05, в частині виготовлення конструкторської документації - стандартам ЕСКД, в частині виготовлення програмної документації - стандартам ЕСПД.

6.5. Навчання користувачів

Проводиться навчання користувачів Порталу всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх

стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

6.6. Комплектування КСЗІ Порталу.

Після виготовлення комплекту технічної документації на КСЗІ Порталу, Виконавець повинен виконати роботи з модернізації та налагодження КСЗІ на території Замовника, на технологічних площадках де розгорнуто Портал.

В рамках розгортання КСЗІ Порталу здійснити постачання компонентів підсистеми криптографічного захисту інформації, які повинні мати дійсні експертні висновки в галузі криптографічного захисту інформації.

Характеристика компонентів підсистеми криптографічного захисту інформації, а також опис їх призначення наведено в Додатках 1,2 до цього документу.

В процесі розробки комплекту експлуатаційної документації, Виконавець повинен виконати роботи по налагодженню елементів КСЗІ згідно проектної документації, та провести попередні випробування з метою встановлення відповідності КСЗІ Порталу прийнятим проектним рішенням на технологічних площадках, де розгорнуті компоненти Порталу.

6.7. Проведення попередніх випробувань КСЗІ Порталу.

Для проведення попередніх випробувань Виконавець повинен розробити та погодити з Замовником програму та методики проведення попередніх випробувань КСЗІ Порталу.

Результати проведення попередніх випробувань КСЗІ Порталу повинні бути оформлені відповідними протоколами. У випадку наявності недоліків (незалежно від того виявлені вони Замовником чи ні), Виконавець повинен виправити їх, та навести докази, що не з’явилися нові недоліки.

Після завершення попередніх випробувань Виконавець повинен скласти протокол проведення попередніх випробувань з рекомендацією щодо подачі заявки на проведення Державної експертизи КСЗІ в сфері технічного захисту інформації. Виконавець повинен супроводжувати роботи по проведенню Державної експертизи до отримання позитивного експертного висновку щодо відповідності КСЗІ вимогам нормативно-правової бази в сфері ТЗІ.

6.8. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань Порталу.

Державна експертиза КСЗІ Порталу проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

Враховуючи, що Виконавець не може проводити Державну експертизу КСЗІ порталу, Виконавець зобов’язаний забезпечити проведення Державної експертизи в галузі технічного захисту інформації КСЗІ Єдиного веб-порталу відкритих даних, оплатити за власний рахунок вартість проведених

Організатором експертних робіт та забезпечити отримання Атестату відповідності, зареєстрованого Державною службою спеціального зв'язку та захисту інформації за підписом уповноваженої особи, який підтверджує, що КСЗІ Порталу, що належить відповідному державному органу, відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у Технічному заданні на створення КСЗІ, та забезпечує захист інформації, що класифікується як конфіденційна інформація, відповідно до вимог нормативних документів з технічного захисту інформації (далі Атестат відповідності).

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Під час побудови КСЗІ Порталу Виконавцю слід передбачити, що Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

6.9. Супроводження КСЗІ

Виконавець повинен забезпечити гарантійне обслуговування компонентів підсистеми криптографічного захисту терміном не менше одного року, а також надати розрахунки її післягарантійного обслуговування та вартість додаткового консультування з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ.

7. ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ДОКУМЕНТАЦІЇ КСЗІ ЄДИНОГО ВЕБ-ПОРТАЛУ ВІДКРИТИХ ДАНИХ

Мінімальний перелік комплекту проектної документації повинен включати:

- відомість технічного проекту;
- пояснювальна записка до технічного проекту;
- опис комплексу технічних засобів;
- опис програмного забезпечення;
- опис організаційної структури.

Мінімальний перелік комплекту експлуатаційної документації повинен включати:

- відомість експлуатаційної документації;
- план захисту;
- -- політика безпеки; правила розмежування доступу;
- інструкція адміністратора безпеки;
- інструкція системного адміністратора;
- інструкція адміністратора баз даних;
- інструкція користувача;
- паспорт-формуляр.

Мінімальний перелік комплекту документації попередніх випробувань повинен включати:

- Програма попередніх випробувань;
- Методика попередніх випробувань;
- Протокол попередніх випробувань.

В документації на КСЗІ ІТС окремими документами, або окремими розділами повинні бути включені наступні відомості:

- інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ;
- порядок введення в експлуатацію КСЗІ;
- порядок модернізації КСЗІ;
- порядок резервування та відновлення інформації в ІТС Фонду;
- порядок відновлення функціонування ІТС Фонду;
- порядок реєстрації користувачів ІТС Фонду;
- порядок надання доступу до ресурсів ІТС Фонду;
- порядок забезпечення антивірусного захисту в ІТС Фонду;
- порядок роботи із засобами криптографічного захисту інформації.

Повний перелік необхідної документації визначається Виконавцем і погоджується із Замовником на етапі проектних робіт по системі в цілому.

Виконавець повинен забезпечити замовника проектами організаційно-розпорядчих документів на створення КСЗІ Порталу.

Мінімальний перелік комплекту документації Експертних випробувань повинен включати:

- Програма експертних випробувань;
- Методика експертних випробувань;
- Протокол експертних випробувань;
- Атестат відповідності.

8. ВИМОГИ ДО ДОКУМЕНТАЦІЇ, ЩО НАДАЮТЬСЯ У СКЛАДІ ТЕХНІЧНОЇ ЧАСТИНИ ДОКУМЕНТАЦІЇ

Технічна частина конкурсної документації повинна містити:

1. Зміст;
2. Перелік скорочень;
3. Схему запровадження підсистеми криптографічного захисту у складі Порталу;
4. Пояснювальна записка до схеми підсистеми криптографічного захисту у складі Порталу;
5. Специфікація обладнання та програмного забезпечення підсистеми криптографічного захисту, що постачається за наступною формою:

№ п/п	Найменування Товару (позначення виробника)	Кіль-ть	Ціна, (грн. з ПДВ)	Вартість, (грн. з ПДВ)

6. Гарантійні зобов’язання на обладнання/програмне забезпечення та умови його гарантійної заміни.
7. Опис послуг, що будуть надано у відповідності до цих Технічних вимог.
8. Копії відповідних експертних висновків за критеріями криптографічного захисту інформації на засоби криптографічного захисту інформації.
9. Документи що підтверджують право на розповсюдження та налаштування засобів криптографічного захисту інформації запропонованих учасником в рамках конкурсної пропозиції.
10. Календарний план надання послуг.

9. ВИМОГИ ДО ВИКОНАННЯ МОНТАЖУ ТА ПУСКОНАЛАГОДЖУВАЛЬНИХ РОБІТ.

Послуги з монтаж та пусконалагоджувальних робіт повинні відповідати вимогам Постанови Кабінету Міністрів України “Про затвердження переліку обов’язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних” від 04.02.1998 №121 та інших нормативних документів, що зазначено у Розділі 8 цього Додатку.

10. ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ

8.1. Закон України «Про інформацію» від 02.10.1992 № 2657 - XII (із змінами і доповненнями);

8.2. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI;

8.3. Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» від 06.07.2010 № 2438-VI;

8.4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI;

8.5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 N 80/94-ВР (із змінами і доповненнями);

8.6. Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV (із змінами і доповненнями);

8.7. Рішення Конституційного Суду України (справа К.Г.Устименка) від 30.10.1997 № 5-зп (Справа № 18/203-97);

8.8. Рішення Конституційного Суду України (справа за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України) від 20.01.2012 № 2-рп/2012 (Справа № 1-9/2012);

8.9. Указ Президента України від 08.07.2009 № 514/2009 «Про доктрину інформаційної безпеки України»;

8.10. Указ Президента України від 24.09.2001 № 891/2001 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних»;

8.11. Указ Президента України від 30.09.2010 № 926/2010 «Про заходи щодо забезпечення пріоритетного розвитку освіти в Україні»;

8.12. Концепція технічного захисту інформації в Україні (із змінами і доповненнями), затверджена постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126;

8.13. Положення про технічний захист інформації в Україні (із змінами і доповненнями), затверджене постановою Кабінету Міністрів України від 27.09.1999 №1229;

8.14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (із змінами і доповненнями), затверджені постановою Кабінету міністрів України від 29.03.2006 № 373;

8.15. Порядок використання комп’ютерних програм в органах виконавчої влади (із змінами і доповненнями), затверджений постановою Кабінету Міністрів України від 10.09.2003 № 1433;

8.16. Загальні вимоги до програмних продуктів, які закуповуються та створюються на замовлення державних органів, затверджені постановою Кабінету Міністрів України від 12.08.2009 № 869;

8.17. Порядок підключення до глобальних мереж передачі даних, затверджений постановою Кабінету Міністрів України від 12.04.2002 № 522;

8.18. Розпорядження Кабінету міністрів України від 02.03.2011 № 192-р «Про затвердження плану заходів проведення у 2011 році Року освіти та інформаційного суспільства»;

8.19. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення, затверджено наказом Держстандарту України від 09.09.93 № 126;

8.20. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення, затверджено наказом Держстандарту України від 11.10.1996 року № 423;

8.21. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт, затверджено наказом Держстандарту України від 19.12.1996 № 511;

8.22. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення, затверджено наказом Держстандарту України від 11.104.1997 № 200;

8.23. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

8.24. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

8.25. ГОСТ 34.602.-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

8.26. ГОСТ 34.603-92 Виды испытаний автоматизированных систем;

8.27. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения;

8.28. РД 50-682-89 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения;

8.29. РД 50-34.698–90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов;

8.30. Комплекс стандартов Единая система конструкторской документации (ЕСКД);

8.31. Наказ Міністерства юстиції України від 30.12.2011 № 3659/5 «Про затвердження Типового порядку обробки персональних даних в базах персональних даних»;

8.32. Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації ДССЗЗІ України від

16.05.2007 N 93, зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087;

8.33. Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затверджений наказом Адміністрації ДССЗЗІ України від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587;

8.34. Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації ДССЗЗІ України від 16.05.2007 № 87, зареєстроване в Міністерстві юстиції України 10.07.2007 за № 785/14052;

8.35. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

8.36. НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

8.37. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБУ від 04.12.2000 № 53;

8.38. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

8.39. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

8.40. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 року № 22 (із зміною №1, затвердженою наказом ДСТСЗІ СБУ від 18.06.2002 № 37);

8.41. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 20 грудня 2000 року № 60;

8.42. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБУ від 08.11.2005 № 125;

8.43. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБУ від 13.12.2002 № 84;

8.44. НД ТЗІ 2.5-010-03 Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 02.04.2003 № 33;

8.45. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 25.03.2011 № 65.

Додаток 1.

Вимоги до компоненти підсистеми криптографічного захисту інформації засоби криптографічного захисту каналів зв'язку

Засоби криптографічного захисту каналів зв'язку (далі – ЗКЗ) повинні забезпечувати конфіденційність та цілісність технологічної інформації користувачів, які здійснюють адміністрування Порталу через незахищене середовище.

ЗКЗ повинні бути представлені у вигляді «криптографічних шлюзів» і «криптографічних клієнтів» та забезпечувати захист каналів зв'язку шляхом побудови віртуальних приватних мереж між «криптографічним шлюзом» і «криптографічними клієнтами» (один до багатьох).

В серверних приміщеннях, де розташовано серверні компоненти Порталу, повинні розміщуватися «криптографічні шлюзи», що реалізують агрегацію віртуальних приватних мереж та відмовостійкість обладнання «криптографічних шлюзів» для створення віртуальних приватних мереж між серверною площадкою (повинен використовуватись «криптографічний шлюз») та площадкою адміністрування (повинен використовуватись «криптографічний клієнт») підрозділами Адміністратора Порталу.

Адміністратор безпеки повинен здійснювати формування ключової системи (ключових даних) для «криптографічних шлюзів» та «криптографічних клієнтів» у необхідній кількості (визначається на етапі технічного проектування системи).

Компоненти ЗКЗ повинні реалізовувати механізми балансування навантаження трафіку та забезпечувати безперервність функціонування захищених каналів зв'язку підсистеми (резервування складових частин ЗКЗ).

Компоненти ЗКЗ повинна реалізовувати загальні функції:

- Захисту даних – забезпечення захисту інформації, яка передається по загальнодоступним мережам, від несанкціонованого ознайомлення й/або модифікації.
- Керування – забезпечення можливості конфігурування та налаштування параметрів компонентів Підсистеми, необхідних для їх функціонування.
- Аудиту – забезпечення можливості проводити аналіз записів у файлах протоколів.
- Ідентифікація й автентифікація – блокування доступу до можливостей керування компонентами ЗКЗ осіб, що не мають відповідних повноважень;
- Захисту функціонування компонентів ЗКЗ від спроб несанкціонованого втручання у їх роботу;
- захист трафіку на рівні аутентифікації / шифрування мережевих пакетів по протоколах IPsec AH і / або IPsec ESP;
- пакетну фільтрацію трафіку з використанням інформації в полях заголовків мережевого і транспортного рівнів;
- контекстну фільтрацію для протоколів TCP і FTP;

- класифікацію та маркування трафіку;
- реалізацію заданого протоколу взаємодії (аутентифікацію та / або захист трафіку) для кожного захищеного з'єднання, доступ в заданому захищеному режимі тільки для зареєстрованих партнерів по взаємодії;
- регульовану стійкість захисту трафіку;
- підтримка NAT Traversal Encapsulation;
- маскування топології сегмента мережі, що захищається (тунелювання трафіку);
- підтримку списку відкликаних сертифікатів (CRL - Certificate Revocation List);
- реєстрація подій, в тому числі і з використанням серверу Syslog;
- надання статистики із використанням протоколів SNMP v.1, v.2c;
- дистанційне та локальне налаштування (за допомогою командної строки або із використанням графічного інтерфейсу);
- підтримка сервісів QoS.

ЗКЗ повинні реалізувати механізми:

- контролю цілісності власного програмного забезпечення;
- тестування на правильність функціонування програмного забезпечення та блокування роботи в разі виявлення порушень;
- захисту від порушення конфіденційності інформації внаслідок помилкових дій оператора або в разі відхилень у роботі складових елементів засобу КЗІ;
- розмежування доступу до функцій засобу КЗІ, криптографічної схеми та ключових даних;
- організації довіреного каналу для отримання інформації, що підлягає захисту;
- знищення ключових даних після закінчення терміну їх дії;
- захисту ключових даних на їх носіях від несанкціонованого зчитування;
- захисту засобу КЗІ від здійснення порушником навмисного зовнішнього впливу;
- захисту від порушення конфіденційності та цілісності ключових даних на ключових документах.

У відповідності до наказу Держспецзв’язку від 20.07.2007 №141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації» засоби КЗІ Підсистеми повинні належати до програмних засобів криптографічного захисту інформації, що мають такі характеристики:

1) вид «А» – засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами, що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів

2) категорії :

- “П” - засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми

криптографічного перетворення інформації, у тому числі засоби імітозахисту та електронного цифрового підпису;

- “Ш” - засоби шифрування інформації ;
- “К” - засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ ;

3) клас «Б2» – відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня).

Засоби КЗІ повинні забезпечувати:

- шифрування інформації за алгоритмом криптографічного перетворення ГОСТ 28147-2009 у режимі гамування зі зворотнім зв’язком;
- мережну автентифікацію учасників захищених обмінів на базі асиметричного криптографічного алгоритму відповідно до ДСТУ-4145-2002;
- підтримку цілісності даних, розрахунок контрольних сум (хешування) – відповідно до ГОСТ 34.311-95;
- генерацію псевдовипадкових послідовностей відповідно до Додатка А ДСТУ 4145-2002;
- протокол розподілу ключових даних відповідно до ДСТУ ISO/IEC 15946-3:2015.

Ключова система засобу криптографічного захисту інформації повинна складатись з довгострокових ключових елементів відповідно до алгоритму, викладеного в ГОСТ 28147-2009. Заповнення ключового запам’ятовуючого пристрою повинно здійснюватися разовими ключовими елементами.

Засоби КЗІ Підсистеми повинні підтримувати роботу таких протоколів передачі даних:

- Authentication Header (IPSec AH);
- Encapsulating Security Payload (IPSec ESP);
- Security Association (IPSec SA);
- Internet Security Association and Key Management Protocol (ISAKMP);
- Internet Key Exchange (IKEv1, IKEv2).

Засоби КЗІ Підсистеми повинні підтримувати роботу в наступних режимах:

- Транспортний (IPSec Transport mode);
- Тунельний (IPSec Tunnel mode).

Пропускна здатність у режимі шифрування для пакетів UDP та TCP– повинна бути не меншою ніж 800 Мбіт\сек.

Додаток 2.

Вимоги до компоненти підсистеми криптографічного захисту інформації, що забезпечують реалізацію механізму автентифікації користувачів системи, обчислення значення електронного цифрового підпису

Компоненти підсистеми криптографічного захисту інформації, що забезпечують реалізацію механізму автентифікації користувачів системи, обчислення значення електронного цифрового підпису ЕЦП (далі – ЗКЗ ЕЦП) повинні забезпечувати: обчислення значення електронного цифрового підпису, авторство інформації в процесі її передачі та обробки.

ЗКЗ ЕЦП призначений для:

- забезпечення виконання функцій накладання електронного цифрового підпису;
- забезпечення виконання функцій перевірки електронного цифрового підпису;
- визначення статусу посилених сертифікатів відкритого ключа;
- отримання позначок часу;
- перевірки позначок часу;
- використання ключових даних від акредитованих центрів сертифікації ключів.

ЗКЗ ЕЦП повинен реалізовувати наступні механізми:

- контроль цілісності програмного забезпечення;
- тестування на правильність функціонування та блокування роботи в разі виявлення порушень;
- захист від порушення конфіденційності інформації внаслідок відхилень у роботі складових елементів Засобу;
- захист від порушення конфіденційності та цілісності ключових даних на ключових документах.

ЗКЗ ЕЦП повинен:

- мати можливість бути використаним у складі будь-якої інформаційної системи, яка реалізована у якості «веб - портального рішення»;
- функціонувати у якості окремої та незалежної частини (модуля) інформаційної системи, яка реалізована у якості «веб - портального рішення» з визначеним переліком функцій та реалізовувати власний прикладний програмний інтерфейс.

ЗКЗ ЕЦП повинен складатись з серверної та клієнтської компонентів у вигляді окремого програмного забезпечення, здатного самостійно виконувати свої функції у повному обсязі, а також функціонувати у середовищі Java Virtual Machine, а також виконуватися скриптами JavaScript.

Серверна компонента повинна забезпечувати:

- інтерфейс взаємодії з інформаційними системами, які реалізовані у якості «веб - портального рішення» за протоколом Simple Object Access Protocol на рівні прикладного програмного інтерфейсу;

- функціонування під управлінням серверу застосунків, який реалізує специфікації Java, а саме Oracle GlassFish Server версії 4.0 та вище або аналог у якості Apache Tomcat;
- реалізацію можливості обчислення електронного цифрового підпису на одержаний від інформаційної системи, яка реалізована у якості «веб - портального рішення» блоку даних;
- реалізацію можливості шифрування одержаного від інформаційної системи, яка реалізована у якості «веб - портального рішення» блоку даних;
- реалізацію можливості розшифрування одержаного від інформаційної системи, яка реалізована у якості «веб - портального рішення» блоку даних;
- реалізацію можливості одержання шифрованого блоку даних від інформаційної системи, яка реалізована у якості «веб - портального рішення» та виконання перевірки електронного цифрового підпису шифрованих даних або здійснення розшифрування даних та виконання перевірки електронного цифрового підпису, що обчислений на шифровані дані та повернення до інформаційної системи, яка реалізована у якості «веб - портального рішення» розшифрованого блоку даних чи інформації про помилку розшифрування блоку даних або помилку перевірки електронного цифрового підпису;
- реалізацію можливості одержання від інформаційної системи, яка реалізована у якості «веб - портального рішення» блоку даних та накладання (обчислення) електронного цифрового підпису з подальшим виконанням шифрування підписаних даних або здійснення шифрування блоку даних отриманого від інформаційної системи, яка реалізована у якості «веб - портального рішення» та виконання обчислення електронного цифрового підпису на шифрований блок даних із поверненням до прикладної системи результату виконання операцій чи інформації про помилку шифрування блоку даних або обчислення електронного цифрового підпису;
- реалізацію можливості отримання за результатом успішної перевірки електронного цифрового підпису, інформації про підписувача, акредитований центр сертифікації ключів, дати та часу підписання;
- реалізацію можливості отримання, за результатом неуспішної перевірки електронного цифрового підпису, інформації про причину такого результату перевірки;
- реалізацію можливості збереження паролю доступу до ключового документу;
- реалізацію можливості виконання операцій з обчислення електронного цифрового підпису, шифрування та розшифрування блоку даних в автоматичному режимі;

- реалізацію можливості перевірки поточного статусу посиленого сертифіката відкритого ключа підписувача (користувача) за механізмом списків відкликаних сертифікатів;
- реалізацію можливості перевірки поточного статусу посиленого сертифіката відкритого ключа підписувача (користувача) за механізмом інтерактивного визначення статусу сертифіката;
- реалізацію можливості перевірки поточного статусу посилених сертифікатів відкритого ключа проміжних та кореневого сертифікатів за механізмом списків відкликаних сертифікатів;
- реалізацію можливості перевірки поточного статусу посилених сертифікатів відкритого ключа проміжних та кореневого сертифікатів за механізмом інтерактивного визначення статусу сертифіката;
- реалізація можливості автоматичного переходу на перевірку статусу посилених сертифікатів відкритого ключа за механізмом списків відкликаних сертифікатів у разі відсутності зв’язку з акредитованим центром сертифікації ключів та обчислення електронного цифрового підпису без використання позначок часу;
- ведення протоколів роботи;
- реалізацію можливості виконання ручного налаштування режимів функціонування.