Прим. № 1

ЗАТВЕРДЖУЮ
Генеральний директор
АТ "ІІТ"
_____ С.Ю. Сінаюк
"19" 12 2012 р.

ЗАТВЕРДЖУЮ
Департамент Державної автомобільної інспекції Міністерства внутрішніх справ України
_____
"20" 12 2012 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на комплексну систему захисту інформації
типового робочого місця зовнішнього користувача
Національної автоматизованої інформаційної системи Департаменту
Державної автомобільної інспекції Міністерства внутрішніх справ України

Шифр "КСЗІ НАІС ДАІ. Клієнт"

ЄААД.468244.149 ТЗ.01

ПОГОДЖЕНО
Адміністрація Державної служби спеціального зв'язку та захисту інформації України
_____ О.Г. Цуркан
"25" 12 2012 р.

Київ 2012 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ДАІ – Державна автомобільна інспекція
ДДАІ – Департамент ДАІ
ДСТУ – Державний стандарт України
ЕЦП – Електронний цифровий підпис
КЗЗ – Комплекс засобів захисту
КЗІ – Криптографічний захист інформації
КМУ – Кабінет Міністрів України
КСЗІ – Комплексна система захисту інформації
КТЗ – Комплекс технічних засобів
МВС – Міністерство внутрішніх справ
НАІС – Національна автоматизована інформаційна система
НД – Нормативний документ
НКІ – Носій ключової інформації
НСД – Несанкціонований доступ
ОС – Операційна система
ОТК – Обов’язковий технічний контроль
ПЗ – Програмне забезпечення
ПК – Програмний комплекс
РС – Робоча станція
СЗІ – Служба захисту інформації
СЧ – Серверна частина
ТЗ – Технічне завдання
ТЗІ – Технічний захист інформації
ЦСК – Центр сертифікації ключів

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому ТЗ застосовуються терміни і визначення, які відповідають встановленим ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни й визначення", Законами України "Про доступ до публічної інформації", "Про захист персональних даних", НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу", НД ТЗІ 2.7-009-09 "Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу", Постановою КМУ від 31.05.2012 №512.

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Повне найменування КСЗІ та її умовне позначення

Комплексна система захисту інформації (КСЗІ) типового робочого місця зовнішнього користувача Національної автоматизованої інформаційної системи (НАІС) Департаменту Державної автомобільної інспекції (ДДАІ) Міністерства внутрішніх справ (МВС) України (далі – НАІС-Клієнт).

1.2 Шифр теми

Шифр КСЗІ: "КСЗІ НАІС ДАІ. Зовнішній користувач".

1.3 Підприємство-замовник та підприємство-виконавець

Замовником та виконавцем є Департамент Державної автомобільної інспекції МВС України. Юридична адреса: 01024, м. Київ, вул. Богомольця, 10. Код ЄДРПОУ: 24521790.

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

Розробка виконується на виконання постанови КМУ "Про затвердження Порядку формування загальнодержавної бази даних про результати обов’язкового технічного контролю транспортних засобів, доступу до неї та встановлення розміру плати за надання таких послуг" від 31.05.2012 №512.

1.5 Відомості про джерела й порядок фінансування робіт

Джерелом фінансування робіт першої черги зі створення КСЗІ (таблиця 8.1) є кошти ДДАІ МВС України. Фінансування робіт другої та третьої черги передбачається за рахунок Організації, що є розпорядником (власником) типових робочих місць зовнішнього користувача в яких створюється КСЗІ.

1.6 Порядок подання результатів робіт

Порядок оформлення та подання результатів роботи із створення КСЗІ у НАІС-Клієнт повинен відповідати вимогам: ДСТУ 3396.0-96, ДСТУ 3396.1-96, РД 50-34.698-90, НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-05.

2 МЕТА Й ПРИЗНАЧЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Мета створення КСЗІ

Метою створення КСЗІ є забезпечення захисту інформації, що обробляється у НАІС-Клієнт, яке являє собою типове робоче місце зовнішніх користувачів, що не є співробітниками підрозділів ДАІ. Захист інформації має здійснюватися шляхом протидії загрозам, які можна очікувати внаслідок дій порушника на всіх технологічних етапах її обробки і в усіх режимах функціонування НАІС-Клієнт.

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.

Для здійснення захисту інформації на всіх стадіях життєвого циклу НАІС-Клієнт у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза обчислювальною системою НАІС-Клієнт;
- програмні засоби (комплекси) захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається у НАІС-Клієнт;
- апаратні (або апаратно-програмні) та програмні засоби (комплекси) криптографічного захисту інформації (далі – КЗІ).

КСЗІ НАІС-Клієнт є типовим модулем, що взаємодіє з інтегрованою КСЗІ у НАІС до якої входить КСЗІ серверної частини НАІС та КСЗІ типових робочих місць внутрішніх користувачів НАІС.

2.2 Функціональне призначення КСЗІ

КСЗІ призначена для:

- реалізації політики безпеки інформації заданої у НАІС-Клієнт;
- ідентифікації та автентифікації користувачів НАІС-Клієнт у ході надання їм доступу до функцій серверної частини НАІС;
- реалізації функцій КЗІ, що передається каналами зв’язку між НАІС-Клієнт та серверною частиною НАІС;
- забезпечення цілісності та доступності відкритої інформації, що обробляється у НАІС-Клієнт, а також конфіденційності та цілісності конфіденційної (персональних даних);
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного оповіщення адміністраторів (уповноважених користувачів) про факти несанкціонованого доступу до інформації;
- ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи НАІС-Клієнт, причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;
- керування засобами захисту інформації, розмежування доступу користувачів до ресурсів НАІС та НАІС-Клієнт, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації;
- 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 НАІС-Клієнт;

- реєстрації, збору, зберігання, обробки даних про події які стосуються обробки інформації з використанням у НАІС-Клієнт та мають відношення до безпеки інформації;
- забезпечення доступності ресурсів НАІС-Клієнт для її користувачів.

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

КСЗІ має розроблятися із врахуванням вимог:

- Закону України "Про міліцію";
- Закону України "Про дорожній рух";
- Закону України "Про інформацію";
- Закону України "Про захист інформації в інформаційно-телекомунікаційних системах";
- Закону України "Про доступ до публічної інформації";
- Закону України "Про захист персональних даних";
- Постанови КМУ "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 р. N 373;
- Постанови КМУ "Про затвердження Порядку формування загальнодержавної бази даних про результати обов’язкового технічного контролю транспортних засобів, доступу до неї та встановлення розміру плати за надання таких послуг" від 31.05.2012 №512;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;
- НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;
- 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.

3 ЗАГАЛЬНА ХАРАКТЕРИСТИКА НАІС-КЛІЄНТ ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ

3.1 Призначення

НАІС-Клієнт – є одномашиним однокористувачевим комплексом до складу якого входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі й технологія її оброблення. Згідно НД ТЗІ 2.5-005-99 НАІС-Клієнт класифікується як ІТС класу "1". НАІС-Клієнт взаємодіє з ІТС НАІС (ІТС класу "3") до якої входить серверна частина НАІС та типові робочі місця користувачів (внутрішніх) НАІС.

3.2 Основні функціональні завдання

НАІС-Клієнт призначене для надання доступу до функцій, що реалізуються серверною частиною НАІС у частині інформаційно-аналітичної підтримки зовнішніх користувачів (клієнтів) НАІС.

На час розробки цього ТЗ (згідно постанови КМУ від 31.05.2012 №512) визначено такі категорії організацій, що виступають у якості зовнішніх користувачів НАІС (далі – Організації-клієнти):

– суб’єкти здійснення обов’язкового технічного контролю (ОТК) транспортних засобів;
– моторне (транспортне) страхове бюро;
– страхові організації, що мають право на здійснення обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів.

3.3 Склад обчислювальної НАІС-Клієнт

3.3.1 Комплекс технічних засобів

До складу комплексу технічних засобів (далі – КТЗ) НАІС-Клієнт відносяться:
– робоча станція (далі – РС);
– апаратно-програмний засіб КЗІ "Електронний ключ "Кристал-1" (далі – АПЗ КЗІ);
– комунікаційне обладнання для підключення до мережі Інтернет (далі – зовнішні телекомунікаційні мережі);
– принтер (необов’язково).

До складу КТЗ НАІС-Клієнт не входять, але взаємодіють із ним через мережу Інтернет – КТЗ веб-серверів зі складу серверної частини НАІС (див. рис. 3.1) .

3.3.2 Програмне забезпечення

Програмне забезпечення (далі - ПЗ) НАІС-Клієнт складається з системного та функціонального програмного забезпечення.

До системного ПЗ НАІС-Клієнт відносяться:
– ОС для РС з лінійки MS Windows;
– ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт";
– ПК антивірусного захисту.

До складу[1] функціонального ПЗ НАІС-Клієнт відносяться:
– ПК "Веб-клієнт".

[1] У складі ПЗ НАІС-Клієнт припускається використовувати додаткове функціональне ПЗ, якщо воно не має функцій взаємодії із серверною частиною НАІС та не створює загроз для інформації, що обробляється у НАІС-Клієнт

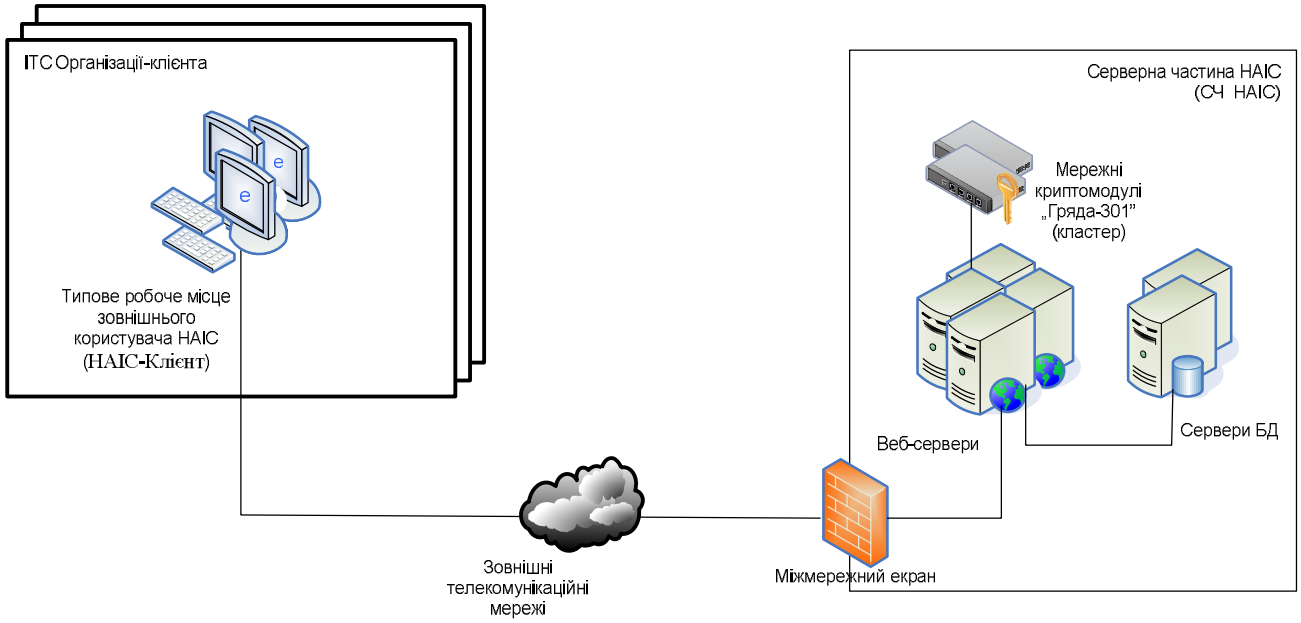

Рисунок 3.1 – Схема взаємодії КТЗ НАІС-Клієнт та КТЗ серверної частини ІТС НАІС

3.4 Характеристика оброблюваної інформації

3.4.1 За змістом вимог щодо захисту, оброблювана інформація поділяється на такі категорії:

– публічна інформація;
– конфіденційна інформація (персональні дані);
– технологічна інформація.

3.4.2 Публічна інформація, що обробляється у НАІС-Клієнт відноситься до відкритої інформації, що є державним інформаційним ресурсом. Публічна інформація є інформацією, вимога щодо захисту якої встановлена Законом. До інформації цієї категорії висуваються підвищені вимоги із забезпечення цілісності та доступності.

3.4.3 Персональні дані, що обробляються у НАІС-Клієнт є інформацією з обмеженим доступом та відноситься до конфіденційної інформації. Персональні дані є інформацією вимога щодо захисту якої встановлена Законом. До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності, цілісності та доступності.

3.4.4 Технологічна інформація складається з технологічної інформація КЗЗ та технологічної інформації щодо адміністрування та управління обчислювальною системою НАІС-Клієнт. До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності та цілісності.

3.5 Середовище користувачів

3.5.1 Категорії користувачів

Користувачі за рівнем повноважень доступу до інформації, що обробляється у НАІС-Клієнт, характеру і змісту робіт, що виконуються у процесі функціонування, поділяються на категорії:

– адміністратори безпеки;
– системні адміністратори;
– клієнти підсистем ПК "Сервер НАІС" (далі – клієнти підсистем).

3.5.2 Функції користувачів категорії "Адміністратор безпеки"

Основними функціями адміністратора безпеки є:
- налаштування КЗЗ складових НАІС-Клієнт;
- аналіз журналів аудиту (реєстрації подій);
- здійснення комплексу дій з контролю цілісності об’єктів захисту;
- оперативне реагування у випадку виникнення подій безпеки інформації.

3.5.3 Функції користувачів категорії "Системний адміністратор"

Основними функціями системного адміністратора є:
- забезпечення працездатності технічного забезпечення НАІС-Клієнт;
- забезпечення працездатності ПЗ (системного та функціонального) НАІС-Клієнт.

3.5.4 Функції користувачів категорії "Клієнти підсистем"

Основними функціями клієнтів підсистем є обробка інформації, що міститься у загальнодержавній базі даних про результати ОТК транспортних засобів (фізично база даних знаходиться на серверах НАІС) у частині:

- внесення інформації про результати ОТК транспортних засобів, яка зазначена в протоколі перевірки технічного стану транспортного засобу чи акті невідповідності технічного стану транспортного засобу;
- внесення інформації про пошкоджені або зіпсовані бланки протоколів перевірки технічного стану транспортного засобу;
- внесення інформації про укладені договори обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів;
- пошуку довідкової інформації, яка необхідна для реалізації покладених функцій з формування загальнодержавної бази даних про результати ОТК транспортних засобів.

3.6 Умови розташування об'єкта

3.6.1 Розміщення обчислювальної системи НАІС-Клієнт має виконуватися, виходячи з:
- локалізації технічних засобів у приміщеннях, фізичний доступ до яких є обмеженим;
- технічних характеристик обладнання і вимог щодо його встановлення і умов експлуатації визначених їх виробником.

3.6.2 Приміщення де розміщуються компоненти НАІС-Клієнт повинні бути розміщені в межах контрольованої території і мати пропускний і внутріоб’єктовий режими, що визначені діючими нормативними та розпорядчими документами керівника Організації-клієнта, де розгортається НАІС-Клієнт.

3.7 Можливі загрози безпеки інформації

Порушення властивостей конфіденційності, цілісності та доступності інформації, що обробляється у НАІС-Клієнт, та спостереженості у НАІС-Клієнт можуть проявлятися внаслідок реалізації загроз, що наведені у таблиці 3.1.

Таблиця 3.1 – Загрози безпеці інформації у НАІС-Клієнт

Властивість інформації, що може бути втрачена / Імовірна загроза безпеці інформації	Конфіденційність	Цілісність	Доступність	Спостережність
1 Загрози об'єктивної природи				
1.1 Пожежа, землетрус, ураган, повінь, різні непередбачувані явища та обставини		+	+	
1.2 Відмови технічних засобів зі складу НАІС-Клієнт		+	+	
1.3 Відмови у мережі енергозабезпечення			+	
2 Загрози суб'єктивної природи				
2.1 Викрадання:				
– технічних засобів;	+	+	+	+
– персональних даних (читання та несанкціоноване копіювання);	+		+	
– технологічної інформації	+	+	+	+
2.2 Модифікація:				
– програмних засобів;	+	+	+	+
– персональних даних;		+	+	
– публічної інформації;		+	+	
– технологічної інформації	+	+	+	+
2.3 Знищення (руйнування):				
– технічних засобів;		+	+	+
– програмних засобів;		+	+	+
– персональних даних;		+	+	
– публічної інформації;		+	+	
– технологічної інформації	+	+	+	+
2.4 Порушення нормальної роботи НАІС-Клієнт внаслідок вичерпання:				
– обсягу вільного дискового простору			+	+
2.5 Помилки:				
– при інсталяції програмного забезпечення;	+	+	+	+
– при написанні спеціального програмного забезпечення;	+	+	+	+
– при експлуатації програмного забезпечення;	+	+	+	+
– при експлуатації технічних засобів	+	+	+	+

4 ВИМОГИ ТА ФУНКЦІЇ КЗЗ НАІС-КЛІЄНТ

4.1 Загальні вимоги до КЗЗ НАІС-Клієнт

Враховуючи реалізовані у НАІС-Клієнт технології обробки інформації, для КЗЗ НАІС-Клієнт висуваються такі загальні вимоги (цілі безпеки):

- КЗЗ НАІС-Клієнт має забезпечити реєстрацію подій, що мають відношення до безпеки;
- КЗЗ НАІС-Клієнт має забезпечити захист від несанкціонованого отримання або викривлення даних початкової ідентифікації та автентифікації користувача;
- КЗЗ НАІС-Клієнт має забезпечити можливість здійснити відновлення компонентів, що були виведенні з ладу у наслідок реалізації атаки чи випадкового збою;
- КЗЗ НАІС-Клієнт має забезпечувати доступ на читання інформації об’єктів захисту тільки для авторизованих користувачів;
- КЗЗ НАІС-Клієнт має забезпечувати доступ на модифікацію інформації об’єктів захисту тільки для авторизованих користувачів;
- КЗЗ НАІС-Клієнт має забезпечувати можливість заміни окремих компонентів НАІС-Клієнт, з мінімально можливим впливом на ефективність роботи користувачів;
- КЗЗ НАІС-Клієнт має забезпечувати захист даних аудиту, що ведеться його компонентами;
- КЗЗ НАІС-Клієнт має забезпечувати захист своїх компонентів від атак спрямованих на вивід їх з ладу;
- КЗЗ НАІС-Клієнт має забезпечувати захист від несанкціонованого перехоплення/викривлення порушником даних, що передаються каналами зв’язку;
- КЗЗ НАІС-Клієнт має реалізовувати політику згідно з якими функції адміністраторів та користувачів відокремлені, а права користувачів надаються у мінімальному обсязі, що дозволяє виконувати посадові обов’язки;
- КЗЗ НАІС-Клієнт має реалізовувати політику ідентифікації та автентифікації, що є захищеною від атак зловмисника типу маскарад.

Функціональну схему КЗЗ НАІС-Клієнт наведено на рисунку 4.1.

4.2 Вимоги до складу КЗЗ НАІС-Клієнт

КЗЗ складається з комплексу технічних засобів (КТЗ) та програмного забезпечення (ПЗ).

4.2.1 До складу КТЗ КЗЗ НАІС-Клієнт має входити апаратно-програмний засіб КЗІ "Електронний ключ "Кристал-1" (АПЗ КЗІ).

4.2.2 До складу ПЗ КЗЗ НАІС-Клієнт мають входити:

- КЗЗ ОС для РС з лінійки MS Windows;
- ПК антивірусного захисту;
- ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт".

4.3 Функції та вимоги до складових (компонентів) КЗЗ НАІС-Клієнт

4.3.1 Функції та вимоги до КЗЗ ОС для РС з лінійки MS Windows:

КЗЗ ОС РС має реалізовувати такі функції:

– забезпечення контролю власної цілісності, цілісності компонентів, пасивних об’єктів та об’єктів-процесів, що функціонують під її керуванням;

– керування атрибутами доступу користувачів та об’єктів;
– ідентифікація та автентифікація користувачів;
– захист від несанкціонованого доступу (НСД) об’єктів захисту, що зберігаються у файловій системі РС;
– захист від повторного використання об’єктів захисту, що знаходяться у оперативній пам’яті РС;
– забезпечення безперервності функціонування ОС;
– ведення журналів аудиту;
– забезпечення можливості адміністрування, керування і підтримки ОС.

4.3.2 Функції та вимоги до ПК антивірусного захисту

ПК антивірусного захисту, що використовуватиметься у складі КЗЗ НАІС-Клієнт повинен мати чинний, позитивний експертний висновок Адміністрації Держспецзв’язку України у сфері ТЗІ.

ПК антивірусного захисту повинен реалізовувати такі функції:
– контроль власної цілісності;
– застосування евристичних методів захисту у процесі викриття шкідливого програмного забезпечення;
– захист файлової системи;
– оновлення антивірусних баз.

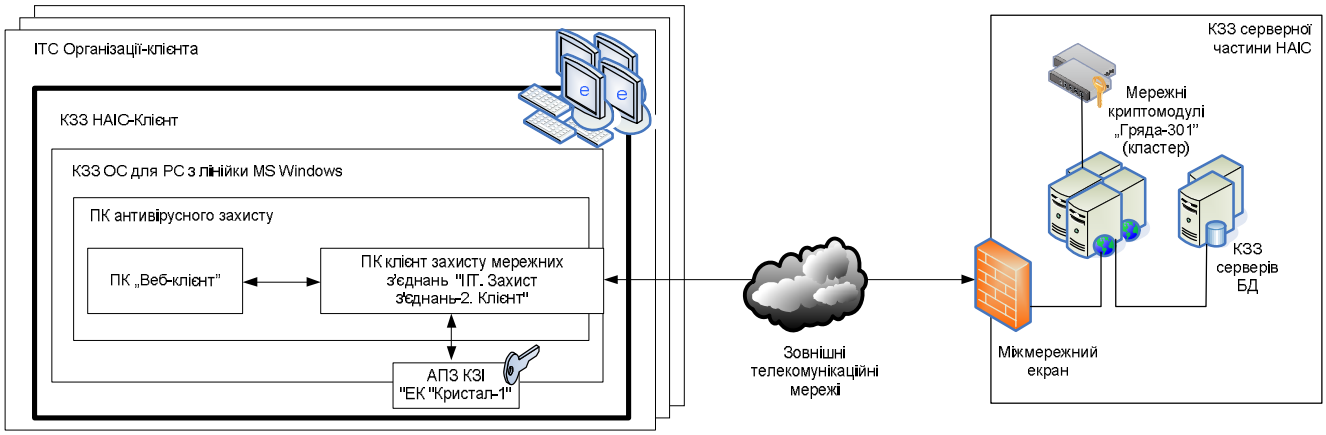

Рисунок 4.1 – Функціональна схема КЗЗ НАІС-Клієнт

4.3.3 Функції та вимоги до ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт"

ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт" повинен мати чинний, позитивний експертний висновок Адміністрації Держспецзв’язку України у сфері КЗІ.

ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт" повинен реалізовувати такі функції:
– реалізація взаємної автентифікації користувача НАІС-Клієнт та КЗЗ серверної частини НАІС при підключенні до серверної частини НАІС;
– встановлення захищеного TCP-з’єднання між ПЗ користувача НАІС-Клієнт та КЗЗ серверної частини НАІС;
– шифрування даних TCP-з’єднання, які передаються між ПЗ користувача НАІС-Клієнт та КЗЗ серверної частини НАІС.

4.3.4 Функції та вимоги до АПЗ КЗІ

У якості АПЗ КЗІ має використовуватися "Електронний ключ "Кристал-1", що має чинний, позитивний експертний висновок Адміністрації Держспецзв'язку України в сфері КЗІ.

АПЗ КЗІ повинен реалізовувати такі функції:

– автентифікація користувачів НАІС-Клієнт перед початком роботи;
– зберігання та захист особистого ключа користувача НАІС-Клієнт;
– апаратна реалізація криптографічних перетворень у складі ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт".

Апаратна реалізація АПЗ КЗІ має забезпечувати захищеність виконання криптографічних перетворень усередині пристрою та унеможливлювати доступ до змісту, та/або можливість несанкціонованого використання особистих ключів користувача з боку ПЕОМ користувача.

4.4 Вимоги до КЗЗ серверної частини НАІС

Вимоги до КЗЗ серверної частини НАІС з якою взаємодіє КЗЗ НАІС-Клієнт викладені у окремому ТЗ: "Технічне завдання на КСЗІ серверної частини НАІС ДДАІ МВС України (ЄААД.468244.148 ТЗ) (шифр "НАІС-Сервер. КСЗІ")".

4.5 Вимоги до КЗІ у НАІС-Клієнт

4.5.1 Функції засобів КЗІ

Засоби КЗІ у НАІС-Клієнт мають забезпечувати виконання таких функцій:
– підтримка механізмів автентифікації користувачів НАІС-Клієнт у серверній частині НАІС;
– забезпечення контролю цілісності підмножини об'єктів НАІС, що визначена політикою безпеки;
– забезпечення авторства для електронних документів та неспростовності джерела даних, що вносяться до БД серверної частини НАІС.

4.5.2 Комплексом засобів КЗІ НАІС-Клієнт повинні використовуватися такі підгрупи ключових даних:
– ключові дані ЦСК;
– ключові дані серверів НАІС;
– ключові дані клієнтів підсистем.

До складу ключових даних ЦСК відносяться сертифікати ЦСК, що використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів тощо.

До складу ключових даних серверів НАІС відносяться їх сертифікати відкритих ключів.

До складу ключових даних клієнтів підсистем відносяться їх особисті ключі та відповідні сертифікати відкритих ключів.

4.5.3 Вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах ЕЦП

У надійних засобах ЕЦП має бути забезпечено застосування положень вимог до форматів даних, структури та протоколів, затверджених Наказом Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453, зареєстрованого в Міністерстві юстиції України 20.08.2012 за № 1398/21710, зокрема:
– вимог до формату посиленого сертифіката відкритого ключа;

– вимог до структури об’єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами;

– вимог до формату списку відкликаних сертифікатів;

– вимог до формату підписаних даних;

– вимог до протоколу фіксування часу;

– вимог до протоколу визначення статусу сертифіката.

5 ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

5.1 Вимоги до КСЗІ в частині захисту від несанкціонованого доступу

5.1.1 У процесі функціонування НАІС-Клієнт об'єктами захисту є: інформаційні ресурси, в яких знаходиться, або може знаходитись інформація, яка підлягає захисту, а також програмне забезпечення (ресурси), що реалізує технології оброблення такої інформації та використовується користувачами НАІС-Клієнт.

5.1.2 Відповідно до функціонального призначення, місця розміщення та виду представлення, політикою безпеки визначається узагальнений перелік інформаційних ресурсів (таблиця 5.1) та програмних ресурсів (таблиця 5.2), які є об’єктами захисту.

Таблиця 5.1 – Узагальнений перелік інформаційних ресурсів

№	Позначення	Назва	Місце обробки[2]		
			ФС	ОП	КПД
1	{Д_ТІК}	Технологічна інформація з адміністрування КЗЗ НАІС-Клієнт	+	+	
2	{Д_ТІУ}	Технологічна інформація управління компонентами НАІС-Клієнт	+	+	
3	{Д_ЖУР}	Журнали аудиту НАІС-Клієнт	+	+	
4	{Д_ВІ}	Публічна інформація (відкрита)	+	+	+
5	{Д_ПД}	Персональні дані	+	+	+
6	{Д_ОК}	Особисті ключі користувачів НАІС-Клієнт[3]			
7	{Д_КШ}	Ключі шифрування (сеансові), які використовуються для захисту даних, що передаються каналами передачі даних		+	

Таблиця 5.2 – Узагальнений перелік програмних ресурсів

№	Позначення	Назва
1	{П_АЗ}	ПК антивірусного захисту
2	{П_ЗК}	ПК клієнт захисту мережних з'єднань "ІІТ. Захист з'єднань-2. Клієнт"
3	{П_ВК}	Програмний комплекс "Веб-клієнт"
4	{П_ОС}	ОС для РС з лінійки MS Windows

5.1.3 Вимоги до користувачів

За рівнем повноважень щодо доступу до програмних комплексів (засобів), інформації, що циркулює та накопичується у НАІС-Клієнт, характером та змістом робіт, які виконуються в процесі функціонування, користувачі НАІС-Клієнт поділяються на такі основні категорії:

– адміністратори безпеки;
– системні адміністратори;
– клієнти підсистем.

Функції користувачів за категоріями наведені у п. 3.5.

Користувачі з роллю "адміністратори безпеки" та/або "системні адміністратори" не мають доступу до функцій, що надаються серверною частиною НАІС.

[2] ФС – файлова система НАІС-Клієнт; ОП – оперативна пам'ять НАІС-Клієнт; КПД – канали передачі даних від НАІС-Клієнт до серверної частини НАІС
[3] Обробляються тільки в АПЗ КЗІ "Електронний ключ "Кристал-1"

5.1.4 Вимоги до взаємодії користувачів і об’єктів захисту НАІС-Клієнт

5.1.4.1 КЗЗ НАІС-Клієнт має реалізовувати довірче керування доступом до об’єктів захисту (п. 5.1.2) з боку користувачів (п. 5.1.3) на основі атрибутів доступу об’єктів захисту та об’єктів-користувачів. Об’єкт-користувач є поданням фізичного користувача у НАІС-Клієнт, що створюється в процесі входження (процедура ідентифікації та автентифікації) користувача у НАІС-Клієнт і характеризується унікальним набором атрибутів (наприклад, ідентифікатором).

5.1.4.2 Категорії об’єктів-користувачів

Категорії об’єктів-користувачів визначаються на основі категорій користувачів:

– об’єкт-користувач категорії "адміністратори безпеки" (К_АБ);
– об’єкт-користувач категорії "системні адміністратори" (К_АС);
– об’єкт-користувач категорії "клієнти підсистем" (К_КП).

5.1.4.3 Атрибути доступу

Атрибути доступу користувачів використовуються для ідентифікації та автентифікації (таблиця 5.3). Атрибути доступу об’єкту-користувача використовуються для ідентифікації та розмежування доступу до об’єктів захисту НАІС-Клієнт (таблиця 5.4). Деякі атрибути одночасно використовуються як користувачами так і відповідними об’єктами-користувачами.

Таблиця 5.3 – Опис атрибутів доступу користувачів (функції ідентифікації та автентифікації)

Назва КЗЗ	Атрибути доступу	Категорії користувачів
КЗЗ {П_ОС}	Логін ОС	Усі категорії користувачів
	Пароль доступу до ОС	Усі категорії користувачів
{П_АЗ}	Пароль до {П_АЗ}	Адміністратори безпеки
КЗЗ серверної частини НАІС (у взаємодії з {П_ЗК})	Логін серверної частини (далі – СЧ) НАІС	Клієнти підсистем
	Пароль доступу до СЧ НАІС	Клієнти підсистем
	АПЗ КЗІ (із особистим ключем)	Клієнти підсистем
	Пароль доступу до АПЗ КЗІ	Клієнти підсистем

Таблиця 5.4 – Опис атрибутів доступу об’єктів-користувачів (функції ідентифікації та розмежування доступу)

Назва КЗЗ	Атрибути доступу	Категорії об’єктів-користувачів
КЗЗ {П_ОС}	Ідентифікатор(-и) облікового запису ОС	К_АБ, К_АС, К_КП
	Ідентифікатор(-и) асоційованої ролі ОС	К_АБ, К_АС, К_КП
{П_АЗ}	Ознака можливості доступу до функцій адміністрування {П_АЗ}	К_АБ
КЗЗ серверної частини НАІС (у взаємодії з {П_ЗК})	Ідентифікатор(-и) облікового запису СЧ НАІС	К_КП
	Ідентифікатор(-и) асоційованих ролей СЧ НАІС	К_КП
	Сертифікат відкритого ключа	К_КП
	IP-адреса НАІС-Клієнт	К_КП
	Шлях до програмного застосування, що використовується для доступу до СЧ НАІС	К_КП

Атрибути доступу об’єктів захисту використовуються КЗЗ НАІС-Клієнт для розмежування доступу до них. Узагальненими переліком атрибутів доступу об’єктів захисту є:

– ідентифікатор (найменування) об’єкту захисту;
– місце розміщення об’єкту захисту;
– асоційований список доступу.

5.1.5 Правила розмежування доступу

КЗЗ НАІС-Клієнт повинен підтримувати такі види доступу об’єктів-користувачів до об’єктів захисту, що є програмними ресурсами як:

– налаштування;
– інсталяція/деінсталяція;
– застосування.

КЗЗ НАІС-Клієнт повинен підтримувати такі види доступу до об’єктів захисту, що є інформаційними ресурсами як:

– читання;
– модифікація (у т.ч. видалення).

Права доступу, що їх має контролювати КЗЗ НАІС-Клієнт, з боку об’єктів-користувачів до програмних ресурсів визначені у таблиці 5.5, а з боку об’єктів користувачів до інформаційних ресурсів – у таблиці 5.6. У таблицях 5.5 та 5.6 вказано максимально можливі права доступу об’єктів-користувачів у НАІС-Клієнт.

Таблиця 5.5 – Права доступу об’єктів-користувачів до програмних ресурсів

№	Об’єкт захисту	Право доступу		
		Налаштування	Інсталяція / Деінсталяція	Застосування
1	{П_АЗ}	К_АБ	К_АС, К_АБ	К_АБ, К_АС, К_КП
2	{П_ЗК}	К_АБ	К_АС, К_АБ	К_КП
3	{П_ВК}	–	К_АС, К_АБ	К_АБ, К_АС, К_КП
4	{П_ОС}	К_АБ, К_АС[4]	К_АС, К_АБ	К_АБ, К_АС, К_КП

Таблиця 5.6 – Права доступу об’єктів-користувачів до інформаційних ресурсів

№	Об’єкт захисту	Право доступу	
		Читання	Модифікація
1	{Д_ТІК}	К_АБ	К_АБ
2	{Д_ТІУ}	К_АБ, К_АС	К_АБ, К_АС
3	{Д_ЖУР}	К_АБ, К_АС	К_АБ[5]
4	{Д_ВІ}	К_КП	К_КП
5	{Д_ПД}	К_КП	К_КП
6	{Д_ОК}	К_КП	–
7	{Д_КШ}	К_КП	–

5.1.6 Принципи розмежування доступу

Усі запити користувачів на доступ до об’єктів захисту повинні оброблятися КЗЗ НАІС-Клієнт. Доступ до пасивного об’єкту захисту має дозволятися/заборонятися згідно правил розмежування доступу за результатами порівняння атрибутів доступу об’єкта-користувача та призначених йому прав.

При розмежуванні доступу до об’єктів захисту, що обробляються в НАІС-Клієнт використовується довірчий принцип керування доступом. КЗЗ НАІС-клієнт надає доступ об’єкту-користувачу до об’єкта захисту, тільки якщо: у асоційованому списку об’єкта захисту для об’єкта-користувача (або ролі до якої він входить) у явному вигляді надано необхідний вид доступу та відсутні заборони на здійснення необхідного виду доступу.

[4] Користувачам категорії К_АС надаються тільки права щодо зміни налаштувань, що не є налаштуваннями безпеки
[5] Під модифікацією мається на увазі право тільки на повне очищення {Д_ЖУР}

5.1.7 Забезпечення безпеки об’єктів захисту у НАІС-Клієнт повинне здійснюватися шляхом комплексного використання організаційних (адміністративних) заходів, правових і законодавчих норм, фізичних і технічних (програмних, апаратно-програмних і апаратних) засобів захисту інформації.

Основні організаційні заходи повинні передбачати:

– створення відповідального підрозділу (або призначення відповідальної за захист інформації особи), якому надаються повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації − служби захисту інформації у НАІС-Клієнт (далі – СЗІ НАІС-Клієнт);

– організацію проведення обстеження середовища функціонування НАІС-Клієнт;

– облік ресурсів системи, що захищаються (інформації, програм тощо), на основі використання відповідних формулярів;

– реалізацію положень політики безпеки інформації у НАІС-Клієнт та надання в установленому порядку адміністраторам безпеки серверної частини НАІС пропозицій щодо внесення у неї змін;

– реалізації плану захисту інформації у НАІС-Клієнт та надання в установленому порядку адміністраторам безпеки серверної частини НАІС пропозицій щодо внесення у нього змін;

– надання адміністратору безпеки серверної частини НАІС інформації для реєстрації нових (блокування/видалення існуючих) облікових записів користувачів НАІС-Клієнт, що мають доступ до серверної частини НАІС;

– порядок проведення відновлювальних робіт і забезпечення безперервного функціонування НАІС-Клієнт;

– порядок проведення модернізації КСЗІ НАІС-Клієнт.

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

– системи нормативно-правового забезпечення робіт із захисту інформації у НАІС-Клієнт;

– процедур доведення до персоналу й користувачів НАІС-Клієнт основних положень політики безпеки інформації, їхнього навчання й підвищення кваліфікації з питань безпеки інформації;

– системи контролю своєчасності, ефективності й повноти реалізації у НАІС-Клієнт рішень із захисту інформації, дотримання персоналом і користувачами положень політики безпеки.

На технічному рівні для блокування загроз НСД до інформаційних ресурсів НАІС-Клієнт необхідне застосування КЗЗ (вимоги, що висуваються та функції складових КЗЗ НАІС-Клієнт наведені у п. 4.3) у складі обчислювальної системи НАІС-Клієнт.

5.1.8 В основу політики безпеки КЗЗ НАІС-Клієнт повинен бути покладений довірчий принцип розмежування доступу до об’єктів захисту.

5.1.9 Розмежування доступу до об’єктів захисту, що зберігаються на машинних носіях великої ємності, має забезпечуватися впровадженням таких організаційних заходів:

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

– фізичний доступ у приміщення де розміщуються компоненти НАІС-Клієнт здійснюється згідно списку та контролюється співробітниками СЗІ;

– склад обчислювальної системи НАІС-Клієнт визначено паспортом-формуляром й його незмінність контролюється адміністратором безпеки;

– у складі програмного забезпечення НАІС-Клієнт відсутні програми, які не призначені для вирішення дозволених функціональних завдань;

– користувачам НАІС-Клієнт заборонено встановлювати будь-яке програмне забезпечення.

5.1.10 У обчислювальній системі компонентів НАІС-Клієнт в процесі роботи розділи і підрозділи системного реєстру повинні бути захищені від змін користувачами. В обов'язковому порядку повинен бути заборонений доступ користувачів до розділів реєстру, які містять дані системи безпеки.

5.1.11 Дозволи користувачам на виконання дій з ресурсами НАІС-Клієнт повинні регулюватися правами доступу. Права доступу визначають правомірність виконання користувачем конкретних дій з ресурсами.

Перелік фізичних осіб, що мають доступ до компонентів НАІС-Клієнт, їх повноваження й службові обов'язки повинні визначатися відповідними розпорядженнями керівництва Організації-клієнта.

5.1.12 У обчислювальній системі НАІС-Клієнт користувач, що намагається одержати доступ до ресурсів, повинен виконати в обов'язковому порядку процедуру входу (реєстрації) у систему. При вході в систему повинна здійснюватися ідентифікація (розпізнавання) і автентифікація (підтвердження автентичності) користувача з використанням атрибутів, що визначені у п. 5.1.4.3.

5.1.13 Незмінність системного й функціонального ПЗ повинна перевірятися при завантаженні системи й забезпечуватися відсутністю засобів модифікації об'єктного коду програм у процесі обробки, а також функціонуванням засобів антивірусного захисту.

5.1.14 Технічний персонал НАІС-Клієнт, постачальники устаткування й фахівці, що здійснюють монтаж і обслуговування технічних засобів НАІС-Клієнт і не мають дозволу на доступ до даних, можуть мати доступ до програмних і апаратних засобів НАІС-Клієнт лише під час робіт з тестування й інсталяції програмного забезпечення, установці й регламентному обслуговуванню устаткування та ін. Зазначені категорії осіб повинні мати дозвіл на доступ тільки до відомостей, які утримуються в програмній і технічній документації на ОС або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

5.1.15 Експлуатація КСЗІ НАІС-Клієнт повинна здійснюватися СЗІ НАІС-Клієнт.

5.2 Визначення функціонального профілю захищеності і рівня гарантій

КЗЗ НАІС-Клієнт має забезпечувати реалізацію такого функціонального профілю захищеності:

{КД-2, КО-1, КВ-1, ЦД-1, ЦВ-1, ДС-1, ДЗ-1, ДВ-1,
НР-2, НИ-2, НИ-3, НК-1, НО-2, НЦ-1, НЦ-2, НТ-2, НВ-1}

Семантика зазначеного профілю прийнята відповідно до НД ТЗІ 2.5-004-99.

КЗЗ НАІС-Клієнт повинен реалізовувати рівень гарантій реалізації послуг безпеки Г-2 згідно з вимогами НД ТЗІ 2.5-004-99.

Специфікації вимог, які визначають правила взаємодії користувачів (об’єктів-користувачів) та захищених об'єктів захисту для кожної послуги, повинні повністю відповідати описам, наведеним у НД ТЗІ 2.5-004-99 з урахуванням того, що взаємодія користувачів (об’єктів-користувачів) та об'єктів захисту НАІС-Клієнт здійснюється відповідно до загальних правил розмежування доступу, атрибутів доступу визначеними у п. 5.1.4.3 та таблицях 5.1 - 5.6 цього ТЗ.

5.3 Вимоги до реалізації послуг забезпечення конфіденційності

КЗЗ НАІС-Клієнт повинен надавати послуги із захисту оброблюваної інформації від несанкціонованого ознайомлення.

5.3.1 Базова довірча конфіденційність (КД-2)

Послуга "Довірча конфіденційність" рівня КД-2 дозволяє користувачу керувати потоками інформації від пасивних об’єктів захисту, що належать до його домену, до інших об’єктів-користувачів, з метою захисту пасивних об’єктів захисту від несанкціонованого ознайомлення з їх вмістом (компрометації).

Політика послуги має відноситися до множини пасивних об’єктів захисту типу {Д_ТІК}, {Д_ТІУ}, {Д_ЖУР}, {Д_ВІ}, {Д_ПД} під час їх обробки як об’єктів файлової системи та користувачів НАІС-Клієнт усіх категорій.

КЗЗ НАІС-Клієнт повинен здійснювати розмежування доступу на підставі атрибутів доступу об’єктів-користувачів і пасивних об’єктів захисту.

КЗЗ НАІС-Клієнт має аналізувати усі запити на доступ від імені об’єктів-користувачів, що надаються з метою одержання інформації, яка міститься в пасивних об’єктах захисту. КЗЗ НАІС-Клієнт має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.6), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ НАІС-Клієнт на підставі атрибутів доступу об’єкта-користувача, що ініціює запит, і пасивного об'єкта захисту.

КЗЗ НАІС-Клієнт повинен надавати можливість[6] користувачам НАІС-Клієнт визначати конкретних користувачів та/або ролі (групи користувачів), які мають право на одержання інформації, що міститься в пасивних об’єктах захисту.

Права користувачів НАІС-Клієнт, на ініціювання та виконання об’єктів-процесів, що можуть бути використані для доступу до пасивних об’єктів захисту, визначені у таблиці 5.5 стовпчик "Застосування". Можливість керування правами на ініціювання, виконання процесів у процесі функціонування НАІС-Клієнт не передбачається.

---

[6] Користувачам К_АБ та К_АС має бути заборонено (за рахунок організаційних заходів) призначати користувачам К_КП права доступу, які є більшими від максимально припустимих (наведені у таблиці 5.6)

Права доступу до кожного об’єкта захисту повинні встановлюватися в момент його створення. Вимог щодо збереження атрибутів доступу пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

5.3.2 Повторне використання об’єктів (КО-1)

Послуга "Повторне використання об’єктів" рівня КО-1 забезпечує коректність повторного використання поділюваних ресурсів (оперативної пам'яті НАІС-Клієнт), гарантуючи, що у випадку, якщо поділюваний ресурс виділяється новому об’єкту-користувачу, він не містить інформації, що залишилася від попереднього об’єкту-користувача.

Політика послуги має відноситися до пасивних об’єктів захисту: {Д_ТІК}, {Д_ТІУ}, {Д_ЖУР}, {Д_ВІ}, {Д_ПД}, {Д_КШ} під час їх обробки у оперативній пам'яті, а також користувачів НАІС-Клієнт усіх категорій.

Перш ніж користувач зможе одержати в своє розпорядження звільнений іншим користувачем об'єкт захисту, встановлені для попереднього користувача права доступу до даного об'єкта захисту мають бути скасовані

Перш ніж користувач зможе одержати в своє розпорядження звільнений іншим користувачем об'єкт захисту, вся інформація, що міститься у даному об'єкті захисту, повинна стати недосяжною.

5.3.3 Мінімальна конфіденційність при обміні (КВ-1)

Послуга "Конфіденційність при обміні" рівня КВ-1 дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Політика послуги, що реалізується КЗЗ НАІС-Клієнт, повинна відноситись до користувачів категорії К_КП та реалізовуватися для пасивних об’єктів захисту: {Д_ВІ} та {Д_ПД} під час їх передачі каналами зв’язку до серверної частини НАІС. При реалізації політики послуги КЗЗ НАІС-Клієнт має використовувати {Д_ОК} та {Д_КШ}.

Політика конфіденційності при обміні, що реалізується компонентами КЗЗ НАІС-Клієнт, повинна реалізовуватись за рахунок використання функцій шифрування за алгоритмом ДСТУ ГОСТ 28147:2009 (режим гамування зі зворотним зв’язком). Користувачі не повинні мати можливості впливати на рівень захисту.

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

5.4 Вимоги до реалізації послуг забезпечення цілісності

КЗЗ НАІС-Клієнт повинен надавати послуги із захисту оброблюваної інформації від несанкціонованої модифікації.

5.4.1 Мінімальна довірча цілісність (ЦД-1)

Послуга "Довірча цілісність" рівня ЦД-1 дозволяє користувачу керувати потоками інформації від пасивних об’єктів захисту, що належать до його домену, до інших об’єктів-користувачів, з метою захисту пасивних об’єктів захисту від несанкціонованої модифікації їх вмісту.

Політика послуги має відноситися до множини пасивних об’єктів захисту типу {Д_ТІК}, {Д_ТІУ}, {Д_ЖУР}, {Д_ВІ}, {Д_ПД} під час їх обробки як об’єктів файлової системи та користувачів усіх категорій.

КЗЗ НАІС-Клієнт повинен здійснювати розмежування доступу на підставі атрибутів доступу об’єктів-користувачів і пасивних об’єктів захисту.

КЗЗ НАІС-Клієнт має аналізувати усі запити на доступ від імені об’єктів-користувачів, що надаються з метою модифікації інформації, яка міститься в пасивних об’єктах захисту. КЗЗ НАІС-Клієнт має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.6), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ НАІС-Клієнт на підставі атрибутів доступу об’єкта-користувача, що ініціює запит, і пасивного об'єкта захисту.

КЗЗ НАІС-Клієнт повинен надавати можливість[7] користувачам НАІС-Клієнт визначати конкретних користувачів та/або ролі (групи користувачів), які мають право на модифікацію інформації, що міститься в пасивних об’єктах захисту.

Права доступу до кожного об’єкта захисту повинні встановлюватися в момент його створення. Вимог щодо збереження атрибутів доступу пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

5.4.2 Мінімальна цілісність при обміні (ЦВ-1)

Послуга "Цілісність при обміні" рівня ЦВ-1 дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Політика послуги, що реалізується КЗЗ НАІС-Клієнт, повинна відноситись до користувачів категорії К_КП та реалізовуватися для пасивних об’єктів захисту: {Д_ВІ} та {Д_ПД} під час їх передачі каналами зв’язку до серверної частини НАІС. При реалізації політики послуги КЗЗ НАІС-Клієнт має використовувати {Д_ОК} та {Д_КШ}.

Політика послуги, що реалізується компонентами КЗЗ НАІС-Клієнт, повинна реалізовуватись за рахунок використання функцій шифрування за алгоритмом ДСТУ ГОСТ 28147:2009 (режим вироблення імітовставки). Користувачі не повинні мати можливості впливати на рівень захисту.

КЗЗ НАІС-Клієнт повинен забезпечувати захист від несанкціонованої модифікації інформації, що міститься в об'єкті, який передається.

5.5 Вимоги до реалізації послуг забезпечення доступності

Апаратні та програмні засоби НАІС-Клієнт повинні надавати послуги забезпечення можливості використання його функцій на прийнятному та зручному для авторизованих користувачів проміжку часу і гарантувати функціонування НАІС-Клієнт у випадку відмови його окремих компонентів.

5.5.1 Стійкість при обмежених відмовах (ДС-1)

Послуга "Стійкість до відмов" рівня ДС-1 дозволяє забезпечити доступність послуг і ресурсів НАІС-Клієнт шляхом забезпечення використання усіх чи окремих функцій НАІС-Клієнт після відмови її компонента.

Політика послуги має відноситися до об’єктів-користувачів (п. 5.1.4) та до АПЗ КЗІ користувачів НАІС-Клієнт.

У разі відмов АПЗ КЗІ, для К_КП стає недоступною послуга ідентифікації та автентифікації засобами КЗЗ НАІС-Клієнт, при цьому така відмова не повинна впливати на можливість проходження процедур ідентифікації та автентифікації для інших користувачів.

КЗЗ повинен повідомляти адміністратора безпеки, у разі виникнення відмови будь-якого з множини об’єктів захисту, що їх стосується політика послуги.

---

[7] Користувачам К_АБ та К_АС має бути заборонено (за рахунок організаційних заходів) призначати користувачам К_КП права доступу, які є більшими від максимально припустимих (наведені у таблиці 5.6)

На етапі технoробочого проектування перелік відмов компонентів НАІС-Клієнт та об’єктів захисту, що їх стосується політика послуги може уточнюватися.

5.5.2 Модернізація (ДЗ-1)

Послуга "Гаряча заміна" рівня ДЗ-1 дозволяє проводити модернізацію {П_ЗК}, {П_АЗ} та АПЗ КЗІ без переривання виконання КЗЗ НАІС-Клієнт функцій захисту.

КЗЗ НАІС-Клієнт має надавати можливість заміни {П_ЗК} на інший засіб КЗІ за умови наявності у останнього експертного висновку Адміністрації Держспецзв'язку у сфері КЗІ та дотримання вимог визначених у ТЗ та технічних умовах на {П_ЗК}, що проходитиме випробування в ході державної експертизи КСЗІ у НАІС-Клієнт.

КЗЗ НАІС-Клієнт має надавати можливість замінити АПЗ КЗІ "Електронний ключ "Кристал-1" на інший апаратно-програмний засіб КЗІ, за умови наявності у останнього експертного висновку Адміністрації Держспецзв'язку у сфері КЗІ та дотримання вимог визначених у ТЗ та технічних умовах на АПЗ КЗІ "Електронний ключ "Кристал-1", що проходитиме випробування в ході державної експертизи КСЗІ у НАІС-Клієнт.

КЗЗ НАІС-Клієнт має надавати можливість замінити {П_АЗ} на інший засіб антивірусного захисту, що має експертний висновок Адміністрації Держспецзв'язку у сфері ТЗІ. При цьому засіб антивірусного захисту на який проводиться заміна має реалізовувати послуги захисту у обсязі та на рівнях визначених для {П_АЗ}, що проходитиме випробування в ході державної експертизи КСЗІ у НАІС-Клієнт.

Модернізація не повинна призводити до переривання виконання КЗЗ НАІС-Клієнт функцій захисту чи проведення додаткової державної експертизи КСЗІ у НАІС-Клієнт.

На етапі технoробочого проектування повинно бути визначено перелік ролей користувачів, які мають право проводити модернізацію та уточено склад компонентів до яких відноситься політика послуги.

5.5.3 Ручне відновлення (ДВ-1)

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

Множиною типів відмов НАІС-Клієнт і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки є:

- відмова програмних компонентів НАІС-Клієнт: {П_АЗ}, {П_ЗК}, {П_ВК} внаслідок порушення цілісності або видалення їх складових (файлів, що виконуються, програмних бібліотек тощо);
- відмова програмних компонентів {П_ОС};
- відмова технічних засобів зі складу НАІС-Клієнт.

Відмови програмних компонентів НАІС-Клієнт мають усуватися шляхом їх повторної інсталяції або заміні пошкоджених складових з еталонної копії.

Відмови програмних компонентів {П_ОС} мають усуватися за рахунок штатних механізмів відновлення, що реалізовані у КЗЗ {П_ОС}.

Відмови технічних засобів зі складу НАІС-Клієнт мають усуватися шляхом заміни на аналогічні моделі.

Після відмови об’єктів, що їх стосується послуга, КЗЗ має перевести відповідні об’єкти до стану, із якого повернути його до нормального функціонування може тільки адміністратор безпеки. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути НАІС-Клієнт до нормального функціонування.

5.6 Вимоги до реалізації послуг забезпечення спостереженості

КЗЗ НАІС-Клієнт повинен надавати послуги із підтримки спроможності НАІС-Клієнт виконувати свої функції, а також із забезпечення відповідальності користувача за свої дії.

5.6.1 Захищений журнал (НР-2)

Послуга "Реєстрація" рівня НР-2 дозволяє контролювати небезпечні для НАІС-Клієнт дії та забезпечити спостереженість за діями користувачів.

КЗЗ НАІС-Клієнт згідно із політикою реєстрації має реєструвати такі події, що мають безпосереднє відношення до безпеки:

- отримання чи спроба отримання користувачем доступу (будь-якого виду) до об’єктів захисту;
- результати ідентифікації та автентифікації користувачів НАІС-Клієнт;
- викриття порушення цілісності або відмова компонентів, що входять до складу НАІС-Клієнт;
- відновлення працездатності компонентів, що входять до складу НАІС-Клієнт;
- зміна атрибутів доступу користувачів НАІС-Клієнт, що знаходяться під керуванням КЗЗ НАІС-Клієнт.

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

Адміністратор безпеки повинен мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Має бути заборонено редагування вмісту журналів реєстрації. Єдиною операцією, що визначена над об’єктам типу журнал реєстрації, що призводить до зміни її вмісту має бути повне очищення. Операції очищення (принаймні останнього) також мають відслідковуватися із використанням журналу реєстрації.

5.6.2 Ідентифікація і автентифікація

5.6.2.1 Загальні вимоги для реалізації послуг рівнів НИ-2 та НИ-3

Послуга "Ідентифікація та автентифікація" рівнів НИ-2 та НИ-3 дозволяє КЗЗ НАІС-Клієнт визначити і перевірити особистість користувача, що намагається одержати доступ до НАІС-Клієнт.

КЗЗ має надавати доступ до функцій НАІС-Клієнт, що запитує користувач, лише після успішного проходження процедури ідентифікації та автентифікації користувачами із використанням відповідних атрибутів. У результаті проходження процедури ідентифікації та автентифікації кожен користувач повинен однозначно ідентифікуватися КЗЗ НАІС-Клієнт. Множина атрибутів, якими характеризуються користувачі наведені у п. 5.1.4.3. Атрибути доступу об’єктів-користувачів мають використовуватися при реалізації таких функціональних послуг захисту, що визначені у профілі захисту визначеного для КЗЗ НАІС-Клієнт як: КД-2, ЦД-1, ДЗ-1, ДВ-1, НР-2, НО-2, НЦ-1, НТ-2.

КЗЗ не повинен передавати та/або зберігати паролі у відкритому вигляді. Замість паролю має використовуватися результат (геш-значення) його перетворення із застосуванням односпрямованих криптографічних функцій – функції гешування. Інформація автентифікації, що передається через канали зв’язку має захищатися із застосуванням протоколів та механізмів КЗІ. КЗЗ НАІС-Клієнт повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

5.6.2.2 Додаткові специфікації послуги "Одиночна ідентифікація і автентифікація" (НИ-2)

Послуга рівня НИ-2 має відноситися до таких користувачів НАІС-Клієнт як: К_АБ, К_АС.

Для користувачів до яких відноситься послуга рівня НИ-2 повинні використовуватися механізми, що забезпечують виконання автентифікації, які ґрунтуються на принципі "знання чогось".

5.6.2.3 Додаткові специфікації послуги "Множинна ідентифікація і автентифікація" (НИ-3)

Послуга рівня НИ-3 має відноситися до таких користувачів НАІС-Клієнт як: К_КП.

Автентифікація К_КП має здійснюватися із застосуванням механізму ЕЦП та {Д_ТІК}.

Для користувачів до яких відноситься послуга рівня НИ-3 повинні використовуватися механізми, що забезпечують виконання автентифікації, які ґрунтуються на двох принципах "знання чогось" та "володіння чимось".

5.6.3 Однонаправлений достовірний канал (НК-1)

Послуга "Достовірний канал" дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ НАІС-Клієнт.

Політика послуги має відноситися до КЗЗ {П_ОС}, КЗЗ {П_ЗК}, КЗЗ {П_АЗ}, користувачів НАІС-Клієнт всіх категорій та їх даних автентифікації.

Встановлення достовірного зв'язку між користувачем, до якого відноситься політика послуги, і КЗЗ НАІС-Клієнт, повинно здійснюватися з використанням захищеного (від перехоплення чи підміни) механізму введення користувачем свого паролю.

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

5.6.4 Розподіл обов'язків адміністраторів (НО-2)

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

Політика розподілу обов’язків повинна визначати адміністративні ролі (адміністратор безпеки, системний адміністратор) та користувальницькі ролі (клієнти підсистем).

Користувач НАІС-Клієнт повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

5.6.5 КЗЗ з контролем цілісності (НЦ-1)

Послуга "Цілісність комплексу засобів захисту" рівня НЦ-1 визначає міру здатності складових КЗЗ НАІС-Клієнт (КЗЗ {П_АЗ} та КЗЗ {П_ЗК}) захищати себе і гарантувати свою здатність керувати захищеними об'єктами.

У якості основного механізму контролю цілісності компонентів, що входять до складу КЗЗ НАІС-Клієнт мають використовуватися:

– механізми контролю цілісності КЗЗ {П_АЗ};
– механізми контролю цілісності, що вбудовані у КЗЗ {П_ЗК}.

У разі виявлення порушення цілісності свого компоненту КЗЗ НАІС-Клієнт повинен повідомити адміністратора безпеки і перевести об’єкт, цілісність якого було порушено, до стану з якого повернути його до нормального функціонування може тільки адміністратор безпеки.

На етапі технороботочого проектування повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ НАІС-Клієнт і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

5.6.6 КЗЗ з гарантованою цілісністю (НЦ-2)

Послуга "Цілісність комплексу засобів захисту" рівня НЦ-2 визначає міру здатності складових КЗЗ НАІС-Клієнт захищати себе і гарантувати свою здатність керувати захищеними об'єктами.

У якості механізму забезпечення цілісності компонентів, що входять до складу КЗЗ НАІС-Клієнт мають використовуватися механізми захисту, що використовуються для реалізації розподілення доменів у КЗЗ {П_ОС}.

КЗЗ {П_ОС} повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування

За допомогою організаційних заходів має бути забезпечено неможливість завантаження НАІС-Клієнт із зовнішніх носіїв або через мережний інтерфейс. На етапі технічного проектування можуть бути уточнені обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ НАІС-Клієнт і всі запити на доступ до захищених об'єктів контролюються КЗЗ НАІС-Клієнт.

5.6.7 Самотестування при старті (НТ-2)

Послуга "Самотестування" рівня НТ-2 дозволяє КЗЗ НАІС-Клієнт перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій НАІС-Клієнт.

Для самотестування повинні використовуватися механізми контролю цілісності, які реалізовані в рамках послуги КЗЗ з контролем цілісності рівня НЦ-1 (див. п. 5.6.5).

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій при запуску на виконання {П_ЗК}, {П_АЗ}. Тести також повинні виконуватися за запитом адміністратора або автоматично при запуску КЗЗ.

5.6.8 Автентифікація вузла (НВ-1)

Послуга "Ідентифікація і автентифікація при обміні" рівня НВ-1 дозволяє КЗЗ НАІС-Клієнт (компонент {П_ЗК} ідентифікувати (встановити і перевірити ідентичність) КЗЗ серверної частини НАІС і забезпечити іншому КЗЗ можливість ідентифікувати себе, перед початком взаємодії. Перш ніж почати обмін з КЗЗ серверної частини НАІС, компонент КЗЗ НАІС-Клієнт повинен автентифікувати КЗЗ серверної частини НАІС із використанням захищеного механізму.

Атрибутами доступу, що мають використовуватися при реалізації послуги повинні бути особистий і відкритий (у складі сертифіката) ключі електронного цифрового підпису КЗЗ, що взаємодіють. Підтвердження ідентичності має здійснюватися на основі затвердженого протоколу автентифікації, що використовує механізм електронного цифрового підпису.

5.7 Вимоги до рівня гарантій

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

6 ВИМОГИ ДО СТАНДАРТИЗАЦІЇ ТА УНІФІКАЦІЇ

6.1 Розробка та функціонування НАІС-Клієнт має проводитись з використанням ліцензійного програмного забезпечення.

6.2 При створенні КСЗІ потрібно керуватися:

- державними стандартами України (ДСТУ);
- нормативними документами системи ТЗІ;
- переліком засобів, дозволених для використання Адміністрацією Держспецзв'язку України.

7 ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ Й ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ

7.1 Проектна документація на комплексну систему захисту інформації повинна включати:

– пояснювальну записку техноробочого проекту КСЗІ у НАІС-Клієнт;

– план захисту інформації у НАІС-Клієнт (сукупність документів), у якому має бути визначено:

- перелік інформації, що підлягає автоматизованому обробленню у НАІС-Клієнт та потребує захисту;
- опис моделі загроз для інформації, оброблюваної у НАІС-Клієнт;
- опис політики безпеки інформації інформації у НАІС-Клієнт;
- перелік організаційно-розпорядчої документації КСЗІ та інших документів, згідно з якими реалізовано захист інформації у НАІС-Клієнт;
- календарний план робіт із захисту інформації у НАІС-Клієнт.

7.2 До складу документації техноробочого проекту повинні входити: основні технічні рішення щодо побудови КСЗІ у НАІС-Клієнт; опис складу КЗЗ; опис функціонування механізмів захисту; способи реалізації послуг безпеки; основні правила експлуатації КЗЗ.

7.3 Склад експлуатаційної документації НАІС-Клієнт:

– положення про службу захисту інформації;

– інструкція про порядок введення та виведення з експлуатації типового робочого місця зовнішнього користувача НАІС;

– програма та методика перевірки відповідності організаційно-технічних рішень реалізованих у КСЗІ на типовому робочому місці зовнішнього користувача НАІС;

- інструкція з модернізації КСЗІ;
- інструкція з резервування та відновлення інформації;
- інструкція з організації контролю за функціонуванням КСЗІ;
- інструкція із забезпечення антивірусного захисту у НАІС-Клієнт;
- інструкція з реєстрації облікових записів для посадових осіб;
- інструкція операторам НАІС (клієнтам підсистем);
- інструкція адміністратору безпеки;
- інструкція системному адміністратору.

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

7.5 Остаточний склад і зміст експлуатаційної документації мають бути уточнені на етапі техноробочого проекту.

7.6 Враховуючи те, що склад і зміст, організаційно-розпорядчої, супровідної, проектної та експлуатаційної документації є типовим, для випадків коли робочі місця зовнішніх користувачів НАІС знаходяться в межах єдиного приміщення (підрозділу) Організації-клієнта у інструкції "Про порядок введення та виведення з експлуатації типового робочого місця зовнішнього користувача НАІС" має бути визначено порядок створення єдиного комплекту документів.

8 ЕТАПИ ВИКОНАННЯ РОБІТ

8.1 Роботи зі створення КСЗІ на типових робочих місцях зовнішніх користувачів НАІС, що знаходяться у розпорядженні (володінні) Організації-клієнта мають здійснюватися у кілька черг.

8.2 Роботи першої черги виконується єдиний раз (див. таблицю 8.1) з метою створення основи для ефективного (за часовими та фінансовими показниками) здійснення подальших робіт зі створення та експертизи КСЗІ у НАІС-Клієнт, які згідно НД ТЗІ 3.7-003-2005 є типовими модулями у складі КСЗІ в НАІС.

Таблиця 8.1 – Зміст та результати робіт першої черги

Стадія	Етапи робіт	Результат роботи
1 Технічне завдання	1.1 Розробка, затвердження та погодження (із Адміністрацією Держспецзв'язку України) ТЗ на створення КСЗІ у НАІС-Клієнт	1 Затверджене та погоджене ТЗ на створення КСЗІ у НАІС-Клієнт
2 Розробка типових організаційно-технічних рішень	2.1 Розробка пропозицій до техноробочого проекту КСЗІ у НАІС-Клієнт. 2.2 Розробка шаблонів для комплекту організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації на КСЗІ у НАІС-Клієнт. 2.3 Розробка інструкції про порядок введення та виведення з експлуатації типового робочого місця зовнішнього користувача НАІС (далі –"Інструкція про порядок …"). 2.4 Розробка "Програми та методики перевірки відповідності організаційно-технічних рішень реалізованих у КСЗІ на типовому робочому місці зовнішнього користувача НАІС" (далі – "Програма та методика…")	1 Пояснювальна записка до техноробочого проекту. 2 Шаблони для комплекту організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації на КСЗІ у НАІС-Клієнт. 3 "Інструкція про порядок …". 4 "Програма та методика…"

8.3 Роботи другої черги (таблиця 8.2) виконуються один раз у кожній Організації-клієнті, що є власником (розпорядником) типових робочих місцях зовнішніх користувачів НАІС.

8.4 Роботи третьої черги (таблиця 8.3) виконуються стосовно кожного НАІС-Клієнта, що знаходиться у розпорядженні (володінні) Організації-клієнта, в якій успішно виконано усі роботи другої черги.

Таблиця 8.2 – Зміст та результати робіт другої черги

Стадія	Етапи робіт	Результат роботи
1 Техно-робочий проект	1.1 Розробка[8] типового комплекту організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації КСЗІ для НАІС-Клієнт, що знаходиться у	1 "Типовий комплект…".

[8] Здійснюється на основі шаблонів документів (п.2.2 таблиця 8.1)

Стадія	Етапи робіт	Результат роботи
	розпорядженні (володінні) Організації-клієнта (далі – "Типовий комплект…"). 1.2 Створення (на основі "Типового комплекту…") організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації КСЗІ для обраного НАІС-Клієнта, що знаходиться у розпорядженні (володінні) Організації-клієнта (далі – НАІС-КОБ). 1.3 Адаптація та погодження "Інструкції про порядок…" та "Програми та методики …"	2 Організаційно-розпорядча, супровідна, робоча та експлуатаційна документація КСЗІ у НАІС-КОБ 3 Погоджені з ДДАІ "Інструкція про порядок…", "Програма та методика …"
2 Введення в дію та перевірка працездатності КСЗІ	2.1 Впровадження заходів захисту та налаштування КЗЗ НАІСК-ОБ керуючись "Інструкцією про порядок…" . 2.2 Проведення попередніх випробувань КСЗІ у НАІС-КОБ керуючись "Програмою та методикою…" . 2.3 Дослідна експлуатація КСЗІ у НАІС-КОБ. 2.4 Корегування організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації КСЗІ у НАІС-КОБ	1 Заходи захисту впроваджені, КЗЗ інстальовані та налаштовані. 2 Акт та протокол попередніх випробувань КСЗІ у НАІС-КОБ. 3 Скорегована організаційно-розпорядча, супровідна, робоча та експлуатаційна документація КСЗІ у НАІС-КОБ. 4 Документація до проведення Державної експертизи
3 Державна експертиза	3.1 Супровід експертних робіт	1 Експертний висновок на типове організаційно-технічне рішення "КСЗІ у НАІС-Клієнт, що знаходиться у розпорядженні (володінні) Організації-клієнта"

Таблиця 8.3 – Зміст та результати робіт третьої черги

Стадія	Етапи робіт	Результат роботи
1 Введення в дію та перевірка відповідності КСЗІ	1.1 Створення (на основі "Типового комплекту…") організаційно-розпорядчої, супровідної, робочої та експлуатаційної документації КСЗІ обраного НАІС-Клієнта. 1.2 Здійснення робіт з введення в експлуатацію обраного НАІС-Клієнта передбачених "Інструкцією про порядок…"	1 Організаційно-розпорядча, супровідна, робоча та експлуатаційна документація КСЗІ обраного НАІС-Клієнта. 2 Протокол випробувань та акт відповідності введеного в експлуатацію НАІС-Клієнта організаційно-технічному рішенню "КСЗІ у НАІС-Клієнт, що знаходиться у розпорядженні (володінні) Організації-клієнта"

9 ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЗ

Зміни і доповнення до ТЗ після його затвердження оформляються окремим доповненням, що затверджується в такому ж порядку, як і це ТЗ.

10 ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ КСЗІ

10.1 Об'єктом випробувань є КСЗІ у НАІС-Клієнт

Метою випробувань є визначення відповідності досягнутого в КСЗІ рівня захищеності інформації вимогам ТЗ і визначення готовності до експлуатації.

10.2 Випробування КСЗІ у НАІС-Клієнт здійснюється з врахуванням змісту етапів та черговості виконання робіт з побудови КСЗІ (п. 8).

10.3 Проводяться наступні види випробувань: попередні, дослідна експлуатація, державна експертиза КСЗІ у НАІС-Клієнт.

10.4 Попередні випробування КСЗІ проводить комісія, яка призначається наказом керівника установи де створюється КСЗІ, відповідно до затвердженої встановленим порядком програми та методики випробувань.

Обсяг випробувань повинен бути достатнім для оцінки всіх показників захисту інформації і вказується в програмі випробувань.

За результатами попередніх випробувань складається акт, у якому зазначаються результати випробувань і дається висновок щодо можливості впровадження КСЗІ у НАІС-Клієнт у дослідну експлуатацію.

10.5 КСЗІ у НАІС-Клієнт вводиться у дослідну експлуатацію згідно з наказом керівника установи де створюється КСЗІ.

10.5.1 Для КСЗІ у НАІС-Клієнт, що створюється у ході виконання робіт другої черги, після завершення дослідної експлуатації складається акт, у якому наведені результати дослідної експлуатації і дається висновок про можливість представлення КСЗІ на державну експертизу.

10.5.2 Для КСЗІ у НАІС-Клієнт, що створюється у ході виконання робіт третьої черги, після завершення дослідної експлуатації складається акт відповідності введеного в експлуатацію НАІС-Клієнта організаційно-технічному рішенню "КСЗІ у НАІС-Клієнт, що знаходиться у розпорядженні (володінні) Організації-клієнта". Затверджені "Акт відповідності …" та відповідні протоколи випробувань є підставою для вводу КСЗІ у НАІС-Клієнт, що створений на конкретному об’єкті інформаційної діяльності Організації-клієнта в експлуатацію.

10.6 Державна експертиза КСЗІ здійснюється організатором експертизи відповідно до «Положення про державну експертизу в сфері технічного захисту інформації», яке затверджено наказом ДССЗЗІ України від 16.05.2007 р. № 93 (із змінами затвердженими наказом Адміністрації Держспецзв’язку України від 10.10.2012 р. № 567).

11 ВИМОГИ ПО ЗАБЕЗПЕЧЕННЮ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОНАННІ РОБІТ

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