ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«13» серпня 2020 р. за № 21773
Дійсний до «13» серпня 2025 р.

Товариство з обмеженою відповідальністю «ДОЛЯ І КО.ЛТД»
(найменування державного органу (організації, підприємства, установи, яким надано Атестат)

засвідчує, що комплексна система захисту інформації
інформаційно-телекомунікаційної системи захищеного вузла інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ»,
(назва ІТС)

що належить **ТОВ «АЙТІ-ІНВЕСТ»,**
(найменування державного органу (організації, підприємства, установи), –

Дніпропетровська обл., м. Кривий Ріг, просп. Гагаріна, 21,
власника (розпорядника) ІТС, місцезнаходження)

забезпечує захист інформації відповідно до вимог нормативних документів з технічного захисту інформації.

Організатор експертизи –

Товариство з обмеженою відповідальністю «ДОЛЯ І КО.ЛТД».
(найменування державного органу (організації, підприємства, установи), що є організатором експертизи)

Експертний висновок на 26 аркушах додається до цього Атестата та є його невід'ємною частиною.

Вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Генеральний директор
ТОВ «ДОЛЯ І КО.ЛТД» _____ **Лариса ТАТАРІНЦЕВА**
підпис ініціали, прізвище

Україна Товариство з обмеженою відповідальністю «ДОЛЯ І КО.ЛТД» Ідентифікаційний код 01043342

Додаток до Атестата відповідності
№ 21773 від «13» серпня 2020 р.

ЕКСПЕРТНИЙ ВИСНОВОК

Комплексна система захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ»

Результати експертизи свідчать, що
комплексна система захисту інформації
(назва комплексної системи захисту інформації)
інформаційно-телекомунікаційної системи
захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ»

що належить **ТОВ «АЙТІ-ІНВЕСТ»,**
Дніпропетровська обл., м. Кривий Ріг, проспект Гагаріна, буд. 21
(назва та адреса організації)
відповідає
(відповідає, не відповідає)

вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі «Технічне завдання на побудову комплексної системи захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ». UA.37214777.00001.КСЗІ.ТЗ».

Вимоги до умов експлуатації (сфери використання) об'єкта експертизи визначені у відповідному розділі цього експертного висновку.

Генеральний директор
ТОВ «ДОЛЯ І КО. ЛТД» — **Лариса ТАТАРІНЦЕВА**
керівник організатора експертизи — підпис — ініціали, прізвище

Україна, Дніпропетровська обл., м. Кривий Ріг, "АЙТІ-ІНВЕСТ", ідентифікаційний код 37214777, з повною відповідальністю

Згідно з оригіналом
Директор ТОВ "Айті-Інвест"
Домнівська

1. ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

Повне найменування об'єкту експертизи: інформаційно-телекомунікаційна система захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ» (далі – ІТС).

КСЗІ побудована відповідно до технічного завдання («Технічне завдання на побудову комплексної системи захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ». UA.37214777.00001.КСЗІ.ТЗ»), погодженого із Адміністрацією Держспецзв'язку.

ІТС являє собою організаційно-технічну систему, яка об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію, в тому числі і технологію її обробки.

За порядком доступу інформація, що циркулює в ІТС, відноситься до конфіденційної (технологічна) та відкритої (транзитна інформація абонентів).

Первинна державна експертиза в сфері технічного захисту інформації КСЗІ ІТС здійснюється з метою оцінки відповідності КСЗІ ІТС вимогам ТЗ, нормативних документів з питань технічного захисту інформації.

Експертні випробування виконуються на підставі рішення Експертної ради з питань державної експертизи в сфері технічного захисту інформації Адміністрації Держспецзв'язку (протокол засідання від 09.07.2020 № 21-2020).

Власником ІТС та виконавцем робіт із створення КСЗІ є ТОВ «АЙТІ-ІНВЕСТ» (50027, Дніпропетровська обл., м. Кривий Ріг, проспект Гагаріна, буд. 21, приміщення 25, код ЄДРПОУ 37214777).

ІТС розташована в приміщенні 13-го поверху будівлі за адресою: м. Кривий Ріг, вул. Мелешкіна 29в, 13 поверх.

Організатором експертизи є ТОВ «ДОЛЯ І КО. ЛТД» (01015, м Київ, пров. Памви Беринди, буд. 4, код ЄДРПОУ 01043342, наказ Адміністрації Держспецзв'язку про видачу ліцензії від 15.02.2017 № 115).

2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1.Призначення ІТС

ІТС призначена для надання органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним та фізичним особам (далі – користувачам) послуг захищеного доступу користувачів до ресурсів та сервісів мережі Інтернет.

2.2.Склад технічних засобів ІТС

ІТС є складною гетерогенною мережею, яка забезпечує надання користувачам (фізичним та юридичним особам) послуг із захищеного доступу до телекомунікаційної мережі загального користування Інтернет.

ІТС використовує технології побудови локальних обчислювальних мереж (Ethernet) та глобальних обчислювальних мереж (TCP/IP). Як фізичне середовище передачі інформаційних сигналів (горизонтальна підсистема

Згідно з оригіналом
Директор ТОВ «АЙТІ-ІНВЕСТ»
Данилевська Н.В.

структурованої кабельної системи) у обчислювальній мережі ІТС використовують волоконно-оптичні лінії зв'язку.

Функціональна схема ІТС наведена на рис. 2.1 (кількість ЕОМ та засобів комутації на функціональній схемі показано умовно).

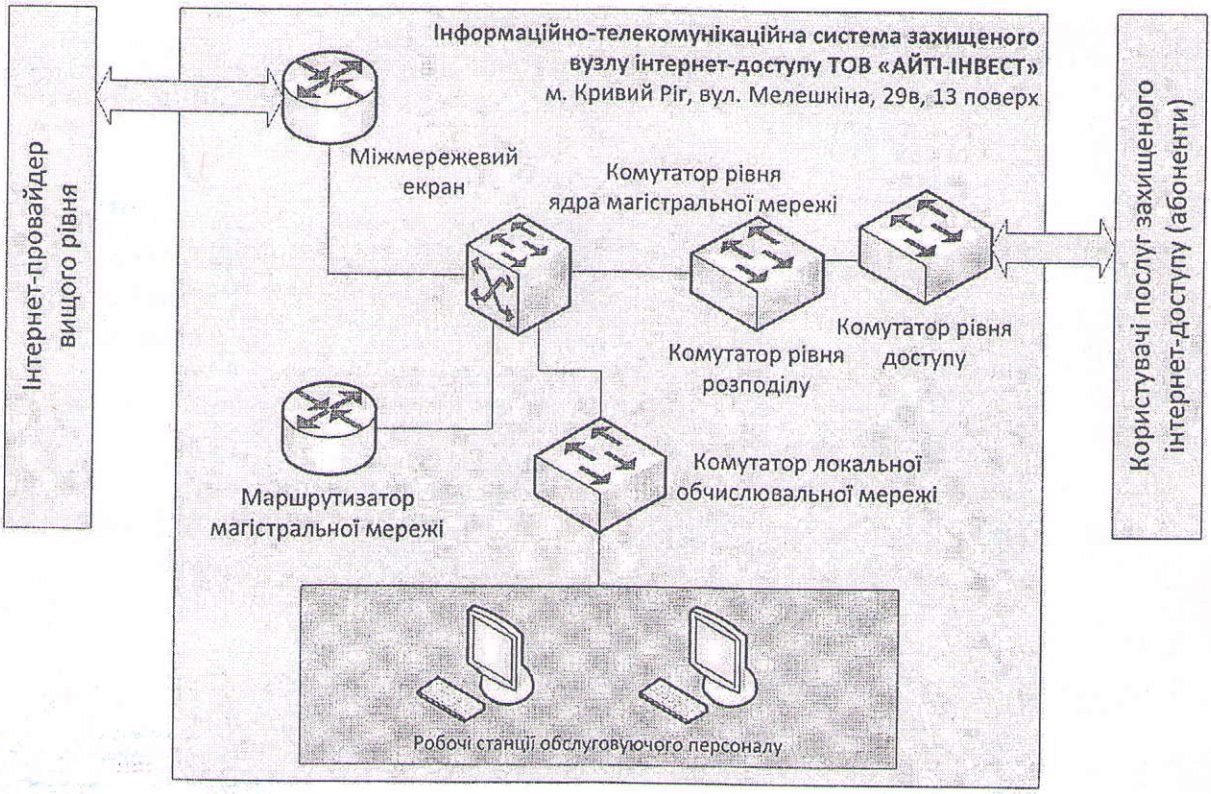

Рис. 2.1. Структурна схема ІТС

До складу ІТС входять наступні технічні засоби (див. рис. 2.1):

1) міжмережевий екран Juniper SRX1500;
2) маршрутизатор магістральної мережі Juniper MX80;
3) комутатор рівня розподілу D-Link DGS 3420-26/28SC;
4) комутатор рівня доступу D-Link DES 3200-10/18/26/28;
5) комутатор рівня ядра магістральної мережі D-Link DXS 3600-32S;
6) комутатор локальної обчислювальної мережі D-Link DES3200-10/26/28/52;
7) робочі станції обслуговуючого персоналу (робочі станції системних адміністраторів, робочі станції чергових інженерів) – 2 шт.

Міжмережевий екран призначений для мережевого захисту ІТС та забезпечує виконання наступних функцій:

– фільтрація та аналіз трафіку з використанням механізмів фільтрації спаму, контентної фільтрації, web-фільтрації, антивірусної фільтрації;
– розмежування доступу між ІТС та зовнішніми мережами;
– інспекція мережевого трафіку та блокування пакетів або сесій, що є підозрілими, з використанням механізмів IPS / IDS;
– маскування топології і мережевих адрес ІТС від публічного перегляду;

Згідно з оригіналом
Директор ТОВ «Айті - Інвест»
Данковська Н.В.

– контроль інформаційних потоків між ІТС та інтернет-провайдерами вищого рівня з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів, в т.ч. атак типу "відмова в обслуговуванні", забезпечення реєстрації, попередження та протидії таким спробам;

– виявлення і протидія мережевим атакам і несанкціонованій мережевій активності;

– фільтрація та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;

– завершення з'єднання з вузлом, у разі атаки;

– протоколювання (реєстрація) подій, що мають відношення до безпеки.

Маршрутизатори магістральної мережі та комутатор рівня ядра магістральної мережі призначені для маршрутизації даних, що передаються в ІТС, на рівні магістральної мережі ІТС.

Комутатори рівнів розподілу та доступу призначені для для забезпечення підключення абонентів до ІТС.

Робочі станції системних адміністраторів використовуються для виконання завдань, пов'язаних з адмініструванням мережевого обладнання ІТС.

Робочі станції чергових інженерів використовуються для виконання завдань, пов'язаних із моніторингом технічних засобів мережі та проведення відповідної діагностики.

Наведені робочі станції обслуговуючого персоналу функціонують під управлінням операційної системи CentOS 7.

Для забезпечення безперебійного живлення технічних засобів ІТС використовуються джерела безперебійного живлення Leoton G4 (2 шт.).

Для зв'язку ІТС з інтернет-провайдерами вищого рівня використовуються волоконно-оптичні лінії зв'язку (із швидкістю обміну даними до 10 Гбіт/с).

Для зв'язку технічних засобів ІТС між собою, а також для зв'язку ІТС з абонентами використовуються волоконно-оптичні лінії зв'язку (із швидкістю обміну даними до 10 Гбіт/с) та лінії зв'язку типу «звита пара» (із швидкістю обміну даними до 100 Мбіт/с).

2.3.Перелік та класифікація інформаційних ресурсів ІТС, порядок обробки та зберігання інформації в ІТС

Узагальнені відомості про інформацію, що обробляється та зберігається в ІТС, наведені в табл. 2.1.

Таблиця 2.1

№ з/п	Вид інформації	Стисла характеристика інформації	Гриф інформації	Вид інформації
1	Транзитна інформація абонентів	Транзитна інформація абонентів, яка передається через ІТС в рамках їх доступу до мережі Інтернет	відкрита	у вигляді IP-пакетів

Згідно з оригіналом
Директор ТОВ "Айті-Інвест"
Данилевська Н.В.

№ з/п	Вид інформації	Стисла характеристика інформації	Гриф інформації	Вид інформації
2	Файли конфігурації програмного та апаратного забезпечення	Списки управління доступом мережевих потоків (Access control lists), що проходять через мережеве обладнання ІТС	конфіденційна (технологічна)	у вигляді файлів
		Конфігураційні налаштування механізмів виявлення та запобігання мережевим атакам		
		Правила політики мережевої безпеки щодо дій при виявленні мережевих аномалій		
		Налаштування технічних засобів ІТС щодо мережевої взаємодії між собою		
		Інші файли конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи ІТС		
3	Журнали реєстрації подій, що ведуться апаратними та програмними засобами ІТС	Зареєстровані події щодо управління даними облікових записів абонентів, щодо надання доступу абонентів до мережі Інтернет, щодо управління конфігураційними налаштуваннями програмного та апаратного забезпечення ІТС, щодо помилок, що виникають в процесі функціонування програмного та апаратного забезпечення ІТС тощо	конфіденційна (технологічна)	у вигляді файлів
4	Файли резервних конфігурацій	Резервні копії файлів конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи ІТС		

Відомості щодо забезпечення властивостей (конфіденційності, цілісності та доступності) інформації, що зберігається та обробляється в ІТС, наведені в табл. 2.2.

Таблиця 2.2

Вид інформації (згідно табл. 2.1)	Відомості щодо забезпечення властивостей інформації		
	конфіденційність	цілісність	доступність
Транзитна інформація абонентів	+	+	+
Файли конфігурації програмного та апаратного забезпечення	+	+	+
Журнали реєстрації подій, що ведуться апаратними та програмними засобами ІТС	+	+	+
Резервні копії файлів конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи ІТС	+	+	+

Згідно з оригіналом
Директор ТОВ «Антіінвест»
Данилевська 11.23

Додатково до наведених в табл. 2.2 видів інформації ІТС здійснює обробку та передачу транзитної інформації абонентів, до якої висуваються вимоги з забезпечення її цілісності та доступності.

За порядком доступу інформація, що циркулює в ІТС, відноситься до конфіденційної (технологічна) та відкритої (транзитна інформація абонентів).

Порядок надання інформаційних послуг та взаємовідносини з абонентами регулюються Правилами надання та отримання телекомунікаційних послуг, затвердженими постановою Кабінету Міністрів України від 11.04.2012 № 295 [НД13], та Основними вимогами до договору про надання телекомунікаційних послуг, затвердженими рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 29.11.2012 № 624. На підставі зазначених документів розроблені форми публічних та письмових договорів з абонентами [3.8]. Зазначені документи містять опис розподілу відповідальності, повноважень, обов'язків та прав провайдера (ТОВ «АЙТІ-ІНВЕСТ») та абонента, зміст зазначених договорів відповідає вимогам нормативних документів

2.4.Фізичне розташування ІТС

ІТС розташована в приміщенні 13-го поверху будівлі за адресою: м. Кривий Ріг, вул. Мелешкіна 29в, 13 поверх.

Власнику ІТС належить право на використання зазначеного приміщення згідно договору про надання колокаційної площі № 1/3-2014 від 01.04.2014.

Серверне приміщення системою охоронної сигналізації та системою відеоспостереження. Доступ персоналу до приміщень здійснюється на підставі наявності ключів від замків дверей відповідних приміщень.

Порядок відвідування приміщень полягає в наданні права доступу до відповідних приміщень керівництву та обслуговуючому персоналу ІТС, функціональними обов'язками якого передбачено необхідність роботи із технічними засобами, розміщеними в цих приміщеннях. Допускається відвідування відповідних приміщень іншими особами (функціональними обов'язками яких не передбачено необхідність роботи із технічними засобами, розміщеними в цих приміщеннях) лише у присутності посадової особи з підрозділу технічної підтримки.

ІТС укомплектована необхідними засобами енергозабезпечення (лінія електроживлення змінного струму 220 В), охоронної сигналізації, допоміжними технічними засобами (кондиціонер), іншими системами життєзабезпечення та відеоспостереження.

2.5.Відомості про користувачів

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

1) системний адміністратор – обслуговуючий персонал, який забезпечує налаштування апаратного та програмного забезпечення технічних засобів для виконання ІТС покладених на неї завдань;

2) черговий інженер (інженер служби технічної підтримки) – обслуговуючий персонал, який здійснює перевірку журналів реєстрації подій,

Згідно з оригіналом
Директор ТОВ «Айті - Інвест»
Данилевська Н. В.

а також перегляд відповідних звітних форм щодо виявлених мережевих аномалій;

3) абонент – фізична або юридична особа, що користується послугами ІТС щодо захищеного доступу до мережі Інтернет.

Обслуговуючий персонал ІТС пройшов підготовку щодо умов та правил використання технічних та програмних засобів, які застосовуються ним під час виконання своїх службових та функціональних обов'язків.

Адміністрування технічних засобів ІТС виконується централізовано системними адміністраторами з використанням відповідних робочих станцій.

2.6.Відомості про склад комплексу засобів захисту інформації від несанкціонованого доступу

До складу *комплексу засобів захисту* (далі – КЗЗ) *ІТС* входять:

- міжмережевий екран Juniper SRX1500;
- маршрутизатор магістральної мережі Juniper MX80;
- комутатор рівня розподілу D-Link DGS 3420-26/28SC;
- комутатор рівня доступу D-Link DES 3200-10/18/26/28;
- комутатор рівня ядра магістральної мережі D-Link DXS 3600-32S;
- комутатор локальної обчислювальної мережі D-Link DES3200-10/26/28/52;
- операційні системи робочих станцій обслуговуючого персоналу CentOS 7.

Відомості щодо реалізації функціональних послуг безпеки окремими складовими КЗЗ ІТС наведені в табл. 2.3.

Таблиця 2.3

КЗЗ	Функціональні послуги безпеки													
	КА-1	КА-2	ЦА-1	ЦА-2	ДС-1	ДР-1	ДЗ-1	ДВ-1	НР-3	НИ-2	НК-1	НО-1	НЦ-1	НТ-2
міжмережевий екран	+	+	+	+		+	+	+	+	+	+	+	+	+
маршрутизатор магістральної мережі	+	+	+	+		+	+	+	+[1]	+	+	+	+	+
комутатор рівня ядра магістральної мережі	+	+	+	+		+	+	+		+	+	+	+	+
комутатор рівня розподілу	+	+	+	+		+	+	+		+	+	+	+	+
комутатори рівня доступу	+	+	+	+		+	+	+		+	+	+	+	+
комутатор локальної обчисловальної мережі	+	+	+	+		+	+	+		+	+	+	+	+
операційні системи робочих станцій обслуговуючого персоналу		+	+				+	+	+[1]	+	+	+	+	+
джерела безперебійного живлення					+									

Примітка: 1) послуга реалізована на рівні НР-2; для реалізації послуги ДС-1 використовуються джерела безперебійного живлення Leoton G4 (2 шт.).

2.7. Інші відомості

Забезпечується безперервне цілодобове функціонування ІТС (окрім

Вірно з оригіналом
Директор ТОВ «Дайті-Інвест»
Данилевська Н.В.

"ДАЙТІ-ІНВЕСТ" ідентифікаційний код 37214777

режиму технічного обслуговування). Виконання робіт, пов'язаних з регламентним технічним обслуговуванням компонентів ІТС, здійснюється у порядку, визначеному відповідною експлуатаційною та технічною документацією.

3. ВИМОГИ НОРМАТИВНИХ ДОКУМЕНТІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, НА ВІДПОВІДНІСТЬ ЯКИМ ЗДІЙСНЮЄТЬСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ

Експертиза КСЗІ здійснювалась з метою визначення відповідності КСЗІ вимогам погодженого із Адміністрацією Держспецзв'язку ТЗ, а також таким нормативним документам системи технічного захисту інформації (далі – НД ТЗІ):

[НД1]. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

[НД2]. Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27.09.1999 № 1229 (зі змінами, унесеними Указом Президента України від 06.10.2000 № 1120).

[НД3]. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373.

[НД4]. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

[НД5]. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

[НД6]. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

[НД7]. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

[НД8]. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

[НД9]. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

[НД10]. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

[НД11]. 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.

[НД12]. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

[НД13]. Правила надання та отримання телекомунікаційних послуг, затверджені постановою Кабінету Міністрів України від 11.04.2012 № 295.

[НД14]. Основні вимоги до договору про надання телекомунікаційних

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Дашевська Н. В.

послуг, затверджені рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 29.11.2012 № 624 (зареєстровано в Міністерстві юстиції України 24.12.2012 за № 2150/22462).

4. МЕТОДИКА ПРОВЕДЕННЯ РОБІТ

Експертні роботи виконувались згідно з розробленими та узгодженими встановленим порядком програмою та методикою державної експертизи у сфері технічного захисту інформації комплексної системи захисту інформації в ІТС.

Програма державної експертизи в сфері технічного захисту інформації комплексної системи захисту інформації захищеного вузлу Інтернет доступу ТОВ «АЙТІ-ІНВЕСТ» (№ 1082/01 від 16.07.2020) та Методика державної експертизи в сфері технічного захисту інформації комплексної системи захисту інформації захищеного вузлу Інтернет доступу ТОВ «АЙТІ-ІНВЕСТ» (№ 1083/01 від 16.07.2020) погоджені із Департаментом захисту інформації Адміністрації Держспецзв'язку.

Програма державної експертизи у сфері технічного захисту інформації додатково погоджена із замовником експертизи (ТОВ «АЙТІ-ІНВЕСТ»).

5. ПЕРЕЛІК ДОКУМЕНТІВ І СПЕЦИФІКАЦІЇ ПРОГРАМНИХ ТА ТЕХНІЧНИХ ЗАСОБІВ, ЯКІ ВИКОРИСТАНО ПРИ ПОБУДОВІ КСЗІ

1. Документація передпроектних робіт:
   - 1.1. Акт обстеження середовищ функціонування інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу.
   - 1.2. Технічне завдання («Технічне завдання на побудову комплексної системи захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ»).
   - 1.3. План захисту інформації. UA.37214777.00001.КСЗІ.ПЗІ.
   - 1.4. Модель загроз інформації. Модель порушника. UA.37214777.00001.КСЗІ.МЗМП.
   - 1.5. Політика безпеки інформації. UA.37214777.00001.КСЗІ.ПБІ.
   - 1.6. Положення про службу захисту інформації. UA.37214777.00001.КСЗІ.ПЛ.
2. Проектна документація:
   - 2.1. «Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.37214777.00001.КСЗІ.ПЗ».
3. Нормативно-розпорядча документація:
   - 3.1. Інструкція системного адміністратора. UA.37214777.00001.КСЗІ.ІІ.
   - 3.2. Інструкція з безпечного використання. UA.37214777.00001.КСЗІ.І2.

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Данилевська Н.В.

3.3. Порядок модернізації і оновлення програмних та апаратних компонентів. UA.37214777.00001.КСЗІ.П1.

3.4. Інструкція про порядок резервування та відновлення інформації. UA.37214777.00001.КСЗІ.І3.

3.5. Інструкція про порядок оперативного відновлення функціонування. UA.37214777.00001.КСЗІ.І4.

3.6. Інструкція про організацію контролю за функціонуванням. UA.37214777.00001.КСЗІ.І5.

3.7. Інструкція про порядок забезпечення антивірусного захисту. UA.37214777.00001.КСЗІ.І6.

3.8. Форми публічних договорів (публічний абонентський договір, договір оренди обладнання для фізичних осіб, регламент тощо).

4. Документація щодо проведених випробувань:

4.1. Програма та методика попередніх випробувань. UA.37214777.00001.КСЗІ.ПМ.

4.2. Протокол попередніх випробувань від 15.07.2020

5. Організаційно-розпорядча документація:

5.1. Наказ про проведення обстеження середовищ функціонування № 140 від 04.06.2020.

5.2. Наказ про створення служби захисту інформації № 141 від 04.06.2020.

5.3. Наказ про проведення попередніх випробувань та дослідної експлуатації КСЗІ ІТС № 144 від 09.07.2020.

5.4. Акт приймання у дослідну експлуатацію КСЗІ ІТС від 16.07.2020.

5.5. Акт завершення дослідної експлуатації КСЗІ ІТС від 17.07.2020.

6. Супровідна документація:

6.1. Формуляр. UA.37214777.00001.КСЗІ.ФО.

7. Експлуатаційна документація на засоби захисту інформації, що входять до складу КЗЗ (у вигляді онлайн-довідки на офіційних веб-сайтах виробників):

7.1. Експлуатаційна документація на міжмережевий екран Juniper SRX1500.

7.2. Експлуатаційна документація на маршрутизатор магістральної мережі Juniper MX80.

7.3. Експлуатаційна документація на комутатор рівня розподілу D-Link DGS 3420-26/28SC.

7.4. Експлуатаційна документація на комутатор рівня доступу D-Link DES 3200-10/18/26/28.

7.5. Експлуатаційна документація на комутатор рівня ядра магістральної мережі D-Link DXS 3600-32S.

7.6. Експлуатаційна документація на комутатор локальної обчислювальної мережі D-Link DES3200-10/26/28/52.

7.7. Експлуатаційна документація на операційні системи робочих станцій обслуговуючого персоналу CentOS 7.

7.8. Експлуатаційна документація на джерела безперебійного живлення Leoton G4.

Згідно з оригіналом
Директор ТОВ "Агмі - Інвест"
Данилевська Н.В.

"АГМІ-ІНВЕСТ" Ідентифікаційний код 37214777

6. РЕЗУЛЬТАТИ ЕКСПЕРТНИХ РОБІТ

Порядок та результати проведення окремих перевірок відповідності об'єкта експертизи вимогам нормативних документів системи ТЗІ за результатами експертних випробувань по кожному пункту методики державної експертизи у сфері технічного захисту інформації КСЗІ в ІТС викладені в документі «Протокол виконання робіт відповідно до розділів 7 – 9 Методики державної експертизи в сфері технічного захисту інформації комплексної системи захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу ТОВ «АЙТІ-ІНВЕСТ».

За результатами перевірок вимог до КСЗІ ІТС отримані такі результати:

6.1. Топологія, склад апаратного та програмного забезпечення ІТС відповідають відомостям, описаним у розділі 2 цього документу та наведеним в проектній документації [2.1] і формулярі ІТС [6.1].

6.2. Здійснено вивчення документації на засоби захисту інформації, що входять до складу КЗЗ ІТС, перевірку правильності їх функціонування та перевірку їх відповідності наданій документації [2.1, 3.1, 7]. За результатами цих робіт встановлено, що задіяні для реалізації задач захисту інформації в КСЗІ механізми захисту інформації зазначених засобів описані в документації [2.1, 3.1, 7] та функціонують у відповідності до наведених у ній положень.

6.3. КСЗІ відповідає вимогам до фізичного середовища, наведеним в ТЗ:

– вхід до приміщень, в яких розміщуються компоненти ІТС, є обмеженим; доступ сторонніх осіб контролюється технічними засобами, двері обладнані механічними замками, охоронною та пожежною сигналізаціями;

– обладнання ІТС розташовується в окремому приміщенні, режим доступу до якого передбачає надання права безперешкодного доступу до таких приміщень лише персоналу ІТС, функціональними обов'язками якого передбачено необхідність роботи із технічними засобами, розміщеними в цих приміщеннях; доступ до цих приміщень сторонніх осіб (осіб, функціональними обов'язками яких не передбачено необхідність роботи із технічними засобами, розміщеними в цих приміщеннях), здійснюється лише у присутності посадової особи, яка відповідає за забезпечення безпеки інформації, яка обробляється та зберігається в ІТС;

– допуск у приміщення та додаткові організаційні заходи із забезпечення безпеки при експлуатації виділених приміщень здійснюються в порядку, визначеному в нормативно-розпорядчій документації власника ІТС з урахуванням заходів щодо реалізації політики безпеки інформації в ІТС [1.5].

6.4. КСЗІ відповідає вимогам до наявності та повноти комплекту технічної документації, визначеним в ТЗ [1.2].

На етапі передпроектних робіт розроблена та оформлена встановленим порядком наступна документація:

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Домбровська Н.В.

– *акт обстеження середовища функціонування* [1.1], в якому зазначені результати проведеного обстеження обчислювальної системи ІТС, інформаційного середовища, фізичного середовища, середовища користувачів, зміст акту відповідає вимогам та рекомендаціям [НД11];

– *опис політики безпеки інформації* [1.5], в якому описані правила, вимоги, обмеження та рекомендації по обробленню інформації, яка потребує захисту в ІТС, дотримання яких забезпечує захист від загроз зазначених у моделі загроз інформації [1.4]; опис відповідає реальним умовам експлуатації ІТС;

– *опис моделі загроз інформації, яка обробляється* в ІТС [1.4], який містить неформалізований опис методів і засобів здійснення загроз для інформації; м*одель порушника* в повної мірі описує можливі цілі, дії та категорії і кваліфікацію порушника [1.4];

– *план захисту інформації* [1.3] містить розділи, визначені в [НД7], які складено з урахуванням умов функціонування ІТС;

– *технічне завдання на створення КСЗІ* в ІТС [1.2] за змістом та оформленням відповідає вимогам, зазначеним в [НД12]; в ТЗ приведено опис характеристик ІТС, викладені вимоги щодо функціонального складу та порядку впровадження програмних і технічних засобів, що забезпечують протидію загрозам та можливостям порушників, які визначені у [1.4] в процесі оброблення інформації в обчислювальній системі ІТС; визначені вимоги до антивірусного захисту інформації, складу проектної та експлуатаційної документації, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою ІТС у доповнення до комплексу програмно-технічних засобів захисту інформації.

У проектній документації на КСЗІ [2.1] наведені рішення, які реалізують вимоги ТЗ [1.2] та політики безпеки, прийнятої в ІТС [1.5].

План захисту інформації [1.3] містить розділи, визначені в [НД7], які складено з урахуванням умов функціонування ІТС.

Порядок експлуатації засобів захисту інформації визначається відповідними інструкцями обслуговуючого персоналу [3.1, 3.2] з урахуванням положень експлуатаційної документації на відповідні засоби [7].

Порядок модернізації існуючих та введення до складу ІТС нових компонентів, наведений у відповідних інструкціях [3.3, 3.4].

Розроблені інструкції та настанови користувачів ІТС описують дії усіх категорій користувачів щодо виконання технологічних операцій з обробки інформації в ІТС, адміністрування та обслуговування КСЗІ, експлуатації комплексу та елементів (складових частин) КЗЗ в повному обсязі [3.1 – 3.7].

Розроблена документація щодо порядку підключення абонентів до ІТС з метою надання їм доступу до мережі Інтернет, яка містить опис порядку підключення абонентів, опис розподілу відповідальності, повноважень, обов'язків та прав оператора (ТОВ «МІРАТЕЛ») та абонента, типові форми заявки та абонентського договору тощо [3.8].

Супровідна (експлуатаційна) документація відповідає вимогам ТЗ [1.2]. Форма та зміст формуляру ІТС [6.1] відповідає вимогам [НД11], реальному складу ІТС.

Документація щодо проведених попередніх випробувань та

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Данівська Н.В.

організаційно-розпорядча документація КСЗІ складена відповідно до положень, зазначених в [НД11]. Ця документація [4.1, 4.2] містить матеріали за результатами проведених попередніх випробувань та дослідної експлуатації ІТС, за висновками, зробленими на цьому етапі, прийнято рішення щодо проведення державної експертизи КСЗІ ІТС.

Всі документи, розроблені при побудові КСЗІ, оформлені, узгоджені та затверджені встановленим порядком, згідно вимог положень чинної нормативно-правової бази в сфері ТЗІ.

Визначені відповідальність, повноваження, обов'язки та права оператора (ТОВ «АЙТІ-ІНВЕСТ») та абонента, розроблені форми публічних та письмових договорів з абонентами [3.8], зміст розроблених договорів відповідає вимогам [НД13, НД14].

Послуги доступу до мережі Інтернет до ІТС надаються інтернет-провайдером вищого рівня – ТОВ «РЕТН» згідно договору № NR-304/18 від 09.11.2018.

Зазначеними договорами визначені відповідальність, повноваження, обов'язки та права наведених інтернет-провайдерів та ТОВ «АЙТІ-ІНВЕСТ», зміст розроблених договорів відповідає вимогам [НД13, НД14].

На ТОВ «АЙТІ-ІНВЕСТ» створено службу захисту інформації та призначено відповідальних осіб за захист інформації [5.2]. Проведено встановленим в [НД10] порядком попередні випробування [5.3] (результати відображені в документі [4.2]) та дослідну експлуатацію КСЗІ [5.4, 5.5].

6.5. КЗЗ ІТС відповідає вимогам ТЗ в частині захисту від НСД:

– все програмне та апаратне забезпечення ІТС проінстальоване (встановлене) коректно та відповідно до положень проектної та експлуатаційної документації [2.1, 3.1], є працездатним, використовується за призначенням та з дотриманням відповідних ліцензійних умов;

– налаштування засобів захисту інформації, що входять до складу КЗЗ, виконано відповідно до положень проектної та експлуатаційної документації [2.1, 3.1];

– міжмережевий екран забезпечує захист ІТС від мережевих атак з боку телекомунікаційних мереж загального користування в обсязі, що відповідає [7.1];

– функції, що виконує міжмережевий екран, відповідають вимогам ТЗ;

– організаційні процедури надання доступу до інформаційних ресурсів ІТС реалізовані коректно згідно [1.5, 3.1];

– процедури контролю за діями користувачів реалізовані коректно згідно [3.6];

– ІТС є працездатною;

– обслуговуючий персонал знає вимоги нормативно-розпорядчих документів на КСЗІ;

– поточний контроль захищеності інформації в ІТС проводиться в повному обсязі, згідно вимог [3.6].

6.6. Персонал ІТС знає вимоги нормативно-розпорядчих документів та порядок використання програмного забезпечення ІТС при виконанні своїх

Згідно з оригіналом
Директор ТОВ „Айті-Інвест"
Дашевська Н.В.

службових обов'язків.

6.7. Антивірусний захист даних, що передаються та обробляються з використанням ІТС, забезпечується на рівні міжмережевого екрану Juniper SRX1500 [2.1].

В документації задокументовано методики управління антивірусним програмним забезпеченням в ІТС в процесі її штатного функціонування згідно наступного [3.7]:

– налаштування безпеки антивірусного програмного забезпечення на міжмережевому екрані відповідають вимогам проектної документації [2.1] та експлуатаційної документації на антивірусне програмне забезпечення;

– антивірусне програмне забезпечення на міжмережевому екрані налаштовано на постійне сканування мережевих об'єктів;

– антивірусне програмне забезпечення є працездатним;

– антивірусні бази повинні оновлюються в порядку, визначеному в [3.7];

– лише системний адміністратор має можливість змінювати системні налаштування антивірусного програмного забезпечення на міжмережевому екрані.

6.8. За результатами перевірки вимог до рівня гарантій встановлено наступне:

– КЗЗ КСЗІ відповідає вимогам до архітектури рівня гарантій Г-2:
  – опис архітектури КЗЗ КСЗІ, наведений в документах [1.2, 2.1], містить необхідний неформальний пояснювальний текст;
  – матеріали проектування КЗЗ КСЗІ містять основні проектні і технічні рішення щодо побудови цих засобів, відомості про склад КЗЗ КСЗІ, функціонування механізмів захисту, способи реалізації послуг безпеки, неформалізований опис механізмів захисту, які використовуються спільно із КЗЗ КСЗІ, взаємодії компонентів КЗЗ КСЗІ та додаткових технічних та організаційних заходів щодо забезпечення функціональних послуг (зазначені відомості наведені в документі [2.1]);
  – компоненти КЗЗ КСЗІ є внутрішньо несуперечливими та утворюють єдине діюче ціле;
  – компоненти КЗЗ КСЗІ у змозі повністю реалізувати встановлену політику безпеки;
  – склад та зміст документів, основні проектні і технічні рішення щодо побудови КЗЗ КСЗІ відповідають вимогам ТЗ;
  – КЗЗ КСЗІ складається з компонент (модулів), які добре визначені та спроектовані як максимально незалежні; кожний з компонентів КЗЗ КСЗІ спроектований відповідно до принципу мінімуму повноважень;
– КЗЗ КСЗІ відповідає вимогам до середовища розробки рівня гарантій Г-2:
  – в процесі розробки:
    - визначені всі стадії життєвого циклу КЗЗ КСЗІ (відображені в документах [1.2, 2.1]);

Згідно з оригіналом
Директор ТОВ "Адмі - Інвест"
Данилевська Н.В.

Дніпропетровська обл., м.Кривий Ріг
"АДМІ ІНВЕСТ"
Ідентифікаційний код 37214777

- розроблені, запроваджені і підтримуються в робочому стані внутрішні документально оформлені методики діяльності на кожній стадії (оформлені у вигляді документу [3.1 – 3.7]);
- документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги (відображені в документах [1.2, 2.1]);

– розробник може повністю керувати конфігурацією КЗЗ КСЗІ, а саме:

- розроблені, запроваджені і підтримуються в робочому стані документовані методики (опис технічних та організаційних заходів) щодо керування конфігурацією КЗЗ КСЗІ на всіх стадіях його життєвого циклу (у вигляді документів [3.1 – 3.7]);
- базова система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення та документацію КЗЗ КСЗІ [3.3];

– базова система керування конфігурацією гарантує постійну відповідність між проектною та експлуатаційною документацією і реалізацією поточної версії КЗЗ КСЗІ [3.1 – 3.7];

– КЗЗ КСЗІ відповідає вимогам до послідовності розробки рівня гарантій Г-2:

– на стадії розробки ТЗ розроблені функціональні специфікації КЗЗ КСЗІ (у вигляді документу [1.2]);
– надані функціональні специфікації включають неформалізований опис політики безпеки, що реалізується КЗЗ КСЗІ [1.5];
– політика безпеки містить перелік і опис послуг безпеки, що надаються КЗЗ КСЗІ [1.5];
– на стадії розробки розроблений неформалізований проект архітектури КЗЗ КСЗІ (відомості відображені в документі [2.1]);
– представлений проект містить перелік і опис компонентів КЗЗ КСЗІ і функцій, що реалізуються ними [2.1];
– розроблений детальний проект КЗЗ КСЗІ, який містить перелік всіх компонентів КЗЗ КСЗІ і опис функціонування кожного механізму (відомості відображені в документі [2.1]);
– на кожній стадії розробки (проектування) існує точний опис КЗЗ КСЗІ і його реалізація точно відповідає вихідним вимогам та політиці безпеки (відомості відображені в документі [2.1]);

– КЗЗ КСЗІ відповідає вимогам до середовища функціонування рівня гарантій Г-2:

– є в наявності і виконуються інструкції інсталяції і ініціалізації КЗЗ КСЗІ, у яких описувані усі параметри конфігурування і можливі обмеження (у складі документу [3.1]);
– передбачено необхідність застосування організаційних і фізичних заходів безпеки, які гарантують, що програмне забезпечення КЗЗ КСЗІ, яке використовується, відповідає безпечній конфігурації (заходи відображені в документах [2.1]);
– передбачено застосування організаційних і фізичних заходів при компіляції програмного забезпечення, які гарантують, що набір механізмів захисту інформації, які реалізують визначену в детальному проекті політику безпеки [2.1], запроваджений в

Згідно з оригіналом
Директор ТОВ «Айті - Інвест»
Данилевська Н. В.

Товариство з обмеженою відповідальністю "АЙТІ-ІНВЕСТ" Ідентифікаційний код 37214777

повному обсязі та функціонує коректно);
- апаратне та програмне забезпечення КЗЗ КСЗІ, яке використовується, відповідає безпечній конфігурації та містить всі необхідні механізми захисту інформації, які реалізують визначену політику безпеки (заходи відображені в документах [3.6]);
- засоби інсталяції, генерації і запуску КЗЗ КСЗІ гарантують, що їх експлуатація починається з безпечного стану (заходи відображені в документі [3.1]);

– КЗЗ КСЗІ відповідає вимогам до документації рівня гарантій Г-2:
- документація відповідає загальним характеристикам, особливостям та реальним умовам технологій обробки інформації КЗЗ КСЗІ [1 – 7];
- в документації наведений опис послуг безпеки, що реалізуються КЗЗ КСЗІ [2.1], настанови адміністратору щодо послуг безпеки [3.1, 3.3 – 3.7], настанови користувачам щодо послуг безпеки [3.2];
- в описі функцій безпеки викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ КСЗІ, а також самі послуги [2.1];
- настанови адміністратору щодо послуг безпеки містять опис засобів інсталяції і запуску КЗЗ КСЗІ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції і запуску КЗЗ КСЗІ, опис властивостей, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ КСЗІ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки [2.1];
- склад і зміст цих документів може забезпечити очікуваний рівень захищеності інформаційних ресурсів КЗЗ КСЗІ;
- настанови користувачу щодо послуг безпеки містять інструкції щодо використання функцій безпеки черговим інженером (не адміністратором) [3.2];
- склад та зміст цих документів відповідають відомостям, наведеним в ТЗ;

– КЗЗ КСЗІ відповідає вимогам до випробувань рівня гарантій Г-2:
- визначені процедури тестування КЗЗ КСЗІ, необхідне оточення і особливі умови, рівень деталізації процедур випробувань, що є достатніми для наступного повторення випробувань, описані очікувані результати кожного тесту [4.1];
- результати випробувань дозволяють оцінити реальну ефективність і повноту проведених випробувань, їх відповідність програмі і методиці, а також, при необхідності, організувати проведення контрольних випробувань [4.2];
- розробником усунені та нейтралізовані всі виявлені при тестуванні «слабкі місця» і виконано повторне тестування КЗЗ КСЗІ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові «слабкі місця»;
- склад та зміст цих документів відповідають відомостям, наведеним в ТЗ [1.2].

Згідно з оригіналом
Директор ТОВ «Айті - Інвест»
Данилевська Н. В.

Україна, Дніпропетровська обл., м. Кривий Ріг
"АЙТІ-ІНВЕСТ"
Ідентифікаційний код 37214777
Товариство з обмеженою відповідальністю

6.9. За результатами перевірки КЗЗ ІТС на відповідність вимогам по захисту інформації від загроз несанкціонованого доступу встановлено, що КЗЗ ІТС коректно реалізує послуги безпеки {КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}, специфікації яких визначені в НД ТЗІ 2.5-004-99, відповідно до вимог ТЗ з урахуванням особливостей їх реалізації, визначених в проектній документації [2.1].

Відомості щодо реалізації функціональних послуг безпеки відповідними компонентами КЗЗ ІТС наведені в табл. 2.1.

За результатами перевірки функціональних послуг безпеки встановлено наступне:

6.9.1. Кожний об'єкт-користувач має наступні атрибути [2.1 (п. 2.7.4)]:

Атрибутами доступу обслуговуючого персоналу, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами КЗЗ, є:

- умовний ідентифікатор в ІТС (логін);
- пароль.

Основними атрибутами доступу абонентів, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами КЗЗ, є MAC-адреса їх мережевого обладнання.

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

- для конфігураційних файлів – ім'я, розширення, атрибути доступу (читання, модифікація, знищення);
- для транзитних мережевих об'єктів – список управління доступом (Access Control List, ACL).

Атрибутами локальних процесів є:

- назва виконуваного програмного модуля;
- ідентифікатор процесу в операційній системі.

Атрибутами мережевих процесів є:

- тип мережевого протоколу (мережевий порт);
- IP-адреса джерела;
- IP-адреса приймальника.

6.9.2. В рамках реалізації *функціональної послуги безпеки «КА-1»* КЗЗ ІТС забезпечує управління доступом мережевих процесів до транзитних мережевих об'єктів згідно налаштованих для них списків управління доступом (Access Control Lists, ACL) [2.1 (п. 2.7.6.1)].

КЗЗ здійснює управління мережевими процесами та розмежовує їх доступ до транзитних мережевих об'єктів на підставі атрибутів процесу і захищеного об'єкта, визначених в п. 6.9.1.

Управління правами доступу транзитних мережевих об'єктів здійснюється системним адміністратором в порядку, визначеному в [3.1], на підставі правил управління доступом, наведених в [1.5].

КЗЗ, склад якого наведений в табл. 2.3, здійснює розмежування доступу мережевих процесів до транзитних мережевих об'єктів у відповідності до правил розмежування доступу, наведених в [1.5, 2.1].

Згідно з оригіналом
Директор ТОВ «АІТІ-Інвест»
Данилевська Н.В.

КЗЗ надає можливість системному адміністратору встановлювати списки контролю доступу таким чином, щоб визначити конкретні мережеві процеси і/або групи процесів, які мають право одержувати інформацію від об'єктів.

Системні адміністратори та чергові інженери мають облікові записи на мережевому обладнанні та в операційних системах робочих станцій обслуговуючого персоналу. Управління такими обліковими записами, групами облікових записів користувачів та їх правами доступу на рівні обчислювальної мережі ІТС здійснюється системним адміністратором [2.1 (п. 2.7.6.1)].

Права доступу до кожного захищеного об'єкта встановлюються в момент його створення [2.1 (п. 2.7.6.1)].

При експорті технологічних об'єктів мережевого обладнання ІТС у вигляді об'єктів файлової системи їх атрибути доступу не зберігаються. Для імпортованих технологічних об'єктів мережевого обладнання ІТС встановлюються налаштовані раніше права доступу до відповідного типу об'єктів [2.1 (п. 2.7.6.1)].

6.9.3. В рамках реалізації *функціональної послуги безпеки «ЦА-2»* КЗЗ ІТС забезпечує управління доступом мережевих процесів до транзитних мережевих об'єктів згідно налаштованих для них списків управління доступом (Access Control Lists, ACL) [2.1 (п. 2.7.6.4)].

КЗЗ здійснює управління мережевими процесами та розмежовує їх доступ до транзитних мережевих об'єктів на підставі атрибутів процесу і захищеного об'єкта, визначених в п. 6.9.1.

Управління правами доступу транзитних мережевих об'єктів здійснюється системним адміністратором в порядку, визначеному в [3.1], на підставі правил управління доступом, наведених в [1.5].

КЗЗ, склад якого наведений в табл. 2.3, здійснює розмежування доступу мережевих процесів до транзитних мережевих об'єктів у відповідності до правил розмежування доступу, наведених в [1.5, 2.1]

КЗЗ надає можливість системному адміністратору встановлювати списки контролю доступу таким чином, щоб визначити конкретні мережеві процеси і/або групи процесів, які мають право модифікувати об'єкти.

Системні адміністратори та чергові інженери мають облікові записи на мережевому обладнанні та в операційних системах робочих станцій обслуговуючого персоналу. Управління такими обліковими записами, групами облікових записів користувачів та їх правами доступу на рівні обчислювальної мережі ІТС здійснюється системним адміністратором [2.1 (п. 2.7.6.1)].

Права доступу до кожного захищеного об'єкта встановлюються в момент його створення [2.1 (п. 2.7.6.4)].

При експорті технологічних об'єктів мережевого обладнання ІТС у вигляді об'єктів файлової системи їх атрибути доступу не зберігаються. Для імпортованих технологічних об'єктів мережевого обладнання ІТС встановлюються налаштовані раніше права доступу до відповідного типу об'єктів [2.1 (п. 2.7.6.4)].

Згідно з оригіналом
Директор ТОВ «Дайті-Інвест»
Дашевська Н.В.

6.9.4. В рамках реалізації *функціональної послуги безпеки «КА-2»* КЗЗ ІТС забезпечує розмежування доступу обслуговуючого персоналу до інформаційних об'єктів, що містять технологічну інформацію компонентів ІТС, де такі об'єкти зберігаються та обробляються [2.1 (п. 2.7.6.2)].

Можливість перегляду цих даних надається обслуговуючого персоналу ІТС на підставі прав доступу кожного користувача, атрибутів користувача і захищеного об’єкта, визначених в п. 6.9.1.

Управління правами доступу обслуговуючого персоналу здійснюється системним адміністратором в порядку, визначеному в [3.1], на підставі правил управління доступом, наведених в [1.5].

КЗЗ, склад якого наведений в табл. 2.3, здійснює розмежування доступу користувачів з ролями «Системний адміністратор», «Черговий інженер» до власних конфігураційних налаштувань у відповідності до правил розмежування доступу, наведених в [1.5, 2.1]. КЗЗ здійснює розмежування доступу до об’єктів захисту на підставі ролей користувачів і групи, до якої віднесено обліковий запис, що встановлені системним адміністратором на рівні обчислювальної мережі ІТС [2.1 (п. 2.7.6.2)].

Системні адміністратори та чергові інженери мають облікові записи на мережевому обладнанні та в операційних системах робочих станцій обслуговуючого персоналу. Управління такими обліковими записами, групами облікових записів користувачів та їх правами доступу на рівні обчислювальної мережі ІТС здійснюється системним адміністратором [2.1 (п. 2.7.6.1)].

Права доступу до кожного захищеного об’єкта встановлюються в момент його створення штатними засобами мережевого обладнання при його розгортанні та налаштуванні системними адміністраторами [2.1 (п. 2.7.6.2)].

– для об’єктів захисту, що є об’єктами файлової системи, – права встановлюються штатними засобами операційної системи при створенні відповідних файлів;

– для технологічної інформації – права встановлюються штатними засобами мережевого обладнання при його розгортанні та налаштуванні системними адміністраторами.

При експорті технологічних об’єктів серверного та мережевого обладнання ІТС у вигляді об’єктів файлової системи їх атрибути доступу не зберігаються. Для імпортованих технологічних об’єктів серверного та мережевого обладнання ІТС встановлюються налаштовані раніше права доступу до відповідного типу об’єктів [2.1 (п. 2.7.6.2)].

6.9.5. В рамках реалізації *функціональної послуги безпеки «ЦА-1»* КЗЗ ІТС забезпечує розмежування доступу обслуговуючого персоналу до інформаційних об'єктів, що містять технологічну інформацію компонентів ІТС, де такі об'єкти зберігаються та обробляються [2.1 (п. 2.7.6.3)].

Можливість модифікації, створення та видалення цих даних надається обслуговуючому персоналу ІТС на підставі прав доступу кожного користувача, атрибутів користувача і захищеного об’єкта, визначених в п. 6.9.1.

Управління правами доступу обслуговуючого персоналу здійснюється системним адміністратором в порядку, визначеному в [3.1], на підставі правил

Вірно з оригіналом
Директор ТОВ «АйТі Інвест»
Дашевська Н.В.

управління доступом, наведених в [1.5].

КЗЗ, склад якого наведений в табл. 2.3, здійснює розмежування доступу користувачів з ролями «Системний адміністратор», «Черговий інженер» до власних конфігураційних налаштувань у відповідності до правил розмежування доступу, наведених в [1.5, 2.1]. КЗЗ здійснює розмежування доступу до об'єктів захисту на підставі ролей користувачів і групи, до якої віднесено обліковий запис, що встановлені системним адміністратором на рівні обчислювальної мережі ІТС [2.1 (п. 2.7.6.3)].

Системні адміністратори та чергові інженери мають облікові записи на мережевому обладнанні та в операційних системах робочих станцій обслуговуючого персоналу. Управління такими обліковими записами, групами облікових записів користувачів та їх правами доступу на рівні обчислювальної мережі ІТС здійснюється системним адміністратором [2.1 (п. 2.7.6.1)].

Права доступу до кожного захищеного об'єкта встановлюються в момент його створення штатними засобами мережевого обладнання при його розгортанні та налаштуванні системними адміністраторами [2.1 (п. 2.7.6.3)]:

При експорті технологічних об'єктів серверного та мережевого обладнання ІТС у вигляді об'єктів файлової системи їх атрибути доступу не зберігаються. Для імпортованих технологічних об'єктів серверного та мережевого обладнання ІТС встановлюються налаштовані раніше права доступу до відповідного типу об'єктів [2.1 (п. 2.7.6.3)].

6.9.6. В рамках реалізації *функціональної послуги безпеки «ДР-1»* КЗЗ ІТС забезпечує можливість управління обсягом ресурсів ІТС, що виділяються користувачу або процесу. Ця послуга розповсюджується на наступні ресурси ІТС [2.1 (п. 2.7.6.5)]:

- кількість одночасних підключень абонентів;
- обмеження кількості одночасних сесій абонентів;
- перепускна здатність каналів передачі даних, що реалізуються ІТС.

Наведені обмеження дозволяють запобігти перевантаженню мережевого обладнання та зберегти працездатність ІТС в моменти пікового навантаження та при проведенні інформаційних атак, спрямованих на зниження стійкості обслуговування.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів ІТС або кількості об'єктів встановлюються системним адміністратором в порядку, наведеному в [3.1].

Спроби користувачів перевищити встановлені обмеження на використання ресурсів реєструються в системному журналі [2.1 (п. 2.7.6.5)].

6.9.7. В рамках реалізації *функціональної послуги безпеки «ДС-1»* КЗЗ ІТС забезпечує стійкість до відмов окремих компонентів ІТС у випадку відмови системи електроживлення на термін до 30 хвилин [2.1 (п. 2.7.6.6)].

Стійкість до відмов зазначених компонентів забезпечується за рахунок використання джерел безперебійного живлення.

Відмова зазначених компонентів не призводить до недоступності послуг, що надаються абонентам.

Технічні засоби КЗЗ мають засоби індикації та/або оповіщення

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Данилевська Н.В.

адміністраторів про відмову системи електроживлення.

Додатково мережеве обладнання ІТС реалізує механізми обробки мережевих пакетів за визначеними пріоритетами, що забезпечує стійкість та надійність передачі інформації абонентів [2.1 (п. 2.7.6.6)].

6.9.8. В рамках реалізації *функціональної послуги безпеки «ДВ-1»* КЗЗ ІТС забезпечує можливість відновлення працездатності відповідних компонент ІТС [2.1 (п. 2.7.6.8)]. Автоматизоване відновлення проводиться у випадків збоїв в роботі системного програмного забезпечення; для цього використовуються штатні засоби відповідних операційних систем мережевого обладнання та операційних систем ЕОМ; в інших випадках проводиться ручне відновлення працездатності, яке здійснюється шляхом заміни несправного обладнання (із дотриманням вимог до реалізації послуги модернізації «ДЗ-1») та відновлення інформації з відповідних резервних копій.

Відмови технічних засобів зі складу ІТС усуваються шляхом заміни на аналогічні або інші моделі, які мають прийнятні характеристики.

Створення резервних копій конфігураційних файлів мережевого обладнання здійснюється шляхом копіювання системним адміністратором відповідних конфігураційних файлів до відповідного каталогу робочих станцій обслуговуючого персоналу [2.1 (п. 2.7.6.8)].

У складі КЗЗ ОС робочих місць обслуговуючого персоналу існують логічні модулі, що реалізують функції моніторингу, які внаслідок збоїв або порушення цілісності файлових систем (системні файли, бібліотеки та налаштування ОС, встановлене ПЗ) переводять відповідний компонент КЗЗ до стану з припиненням обслуговування, з якого повернути в режим нормального функціонування може користувач з адміністративною роллю за допомогою ручних (неавтоматизованих) процедур. Механізми засобів розмежування доступу КЗЗ ОС надають можливість повернення до нормального функціонування шляхом перезапуску відповідних компонентів або їх відновлення з оперативних та архівних резервних копій лише після підтвердження системним адміністратором [2.1 (п. 2.7.6.8)].

У складі КЗЗ мережевого обладнання існують логічні модулі, що реалізують функції моніторингу, які внаслідок збоїв або порушення цілісності їх ОС (системні файли, бібліотеки та налаштування ОС) переводять відповідний компонент КЗЗ до стану з припиненням обслуговування, з якого повернути в режим нормального функціонування може користувач з адміністративною роллю за допомогою ручних (не автоматизованих) процедур. Механізми засобів розмежування доступу КЗЗ мережевого обладнання надають можливість повернення до нормального функціонування шляхом перезапуску відповідних компонентів або їх відновлення з оперативних та архівних резервних копій лише після підтвердження системним адміністратором [2.1 (п. 2.7.6.8)].

Порядок виконання процедур відновлення працездатності ІТС та інформації, а також повноваження адміністраторів щодо відновлення інформації, та процедури повернення ІТС до нормального функціонування, визначений в експлуатаційній документації [3.4, 3.5].

Відновлення працездатності здійснюється системним адміністратором в порядку, визначеному в документах [3.4, 3.5].

Згідно з оригіналом
Директор ТОВ «Інті-Інвест»
Данівська Н.В.

6.9.9. В рамках реалізації *функціональної послуги безпеки «ДЗ-1»* КЗЗ ІТС забезпечує можливість модернізації системного програмного забезпечення, яке може бути оновлено без переривання обслуговування [2.1 (п. 2.7.6.8)].

Модернізація іншого програмного забезпечення, у тому числі і оновлення антивірусних баз антивірусного програмного забезпечення, а також апаратного забезпечення ІТС, не впливає на технологію обробки інформації або рівень її захищеності. Так, включення до складу компоненту ІТС додаткових одиниць ідентичних або аналогічних за функціональним призначенням технічних засобів (за умови наявності у обладнання, що замінюється, експертного висновку за результатами державної експертизи в сфері технічного захисту інформації) здійснюється у випадках необхідності розширення та (або) покращення експлуатаційних можливостей (характеристик) компоненту ІТС. Зміна місця розміщення технічного засобу здійснюється у випадку необхідності зміни розміщення компоненту ІТС, пов'язаної з аварійним станом приміщення, де розміщено компонент ІТС, проведенням ремонтних, будівельно-монтажних робіт у приміщенні тощо.

Зміна складу технічних засобів ІТС в наведеному вище обсязі не потребує проведення додаткової державної експертизи в сфері технічного захисту інформації. В іншому випадку зміна складу технічних засобів ІТС потребує проведення додаткової державної експертизи в сфері технічного захисту інформації [3.3].

Така модернізація здійснюється системним адміністратором ІТС в порядку, визначеному в документі [3.3].

6.9.10. В рамках реалізації *функціональної послуги безпеки «НР-3»* КЗЗ ІТС забезпечує реєстрацію наступних подій [2.1 (п. 2.7.6.9)]:

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

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

– отримання або намагання отримання доступу користувачем будь якої категорії до будь-яких захищених процесів і об'єктів ІТС;

– реєстрація подій, пов'язаних зі зміною конфігурації налаштувань компонентів системи;

– зміна прав доступу до об'єктів захисту;

– спроби використання обчислювальних ресурсів ІТС з перевищенням встановлених квот.

Визначені події реєструються у вигляді записів у системних журналах подій, засобах аудиту прикладного програмного забезпечення (далі – журнали реєстрації), інших електронних журналах мережевого обладнання та операційних систем ЕОМ, які містять інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Наведена у журналах реєстрації інформація є достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події [2.1 (п. 2.7.6.9)].

Адміністратори проводять аналіз зареєстрованих подій в порядку, визначеному в [3.6].

Згідно з оригіналом
Директор ТОВ "АЙТІ-ІНВЕСТ"
Данилевська Н. В.

"АЙТІ-ІНВЕСТ" Ідентифікаційний код 37214777

КЗЗ забезпечує захист журналів реєстрації від несанкціонованого доступу. Переглянути журнал реєстрації подій має право лише системний адміністратор та черговий інженер [2.1].

Міжмережевий екран забезпечує можливість формування та відправлення адміністратору службових повідомлень про виявлені спроби інформаційних атак, спрямованих на отримання доступу (вторгнення) до локальної мережі, яка захищається з використанням шлюзу. З цією метою в шлюзі реалізована та застосовується системи запобігання вторгненням (Intrusion Prevention System, IDS), яка призначена для виявлення шкідливої активності, що може порушити інформаційну безпеку. До такої активності належать мережеві атаки проти вразливих мережевих служб (сервісів), спрямовані на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дій шкідливого програмного забезпечення (комп'ютерних вірусів, троянів тощо). Виявлення порушень безпеки здійснюється з використанням політик безпеки, які визначають евристичні правила пошуку та правила аналізу сигнатур відомих інформаційних атак [2.1, 7.1].

Політики безпеки, які налаштовуються в міжмережевому екрані, дозволяють визначити критичний рівень порушень безпеки, при досягненні якого інформаційна атака блокується (шляхом блокування певного мережевого протоколу, TCP-порту або IP-адреси комп'ютера, з якого проводиться атака) [2.1, 7.1].

6.9.11. В рамках реалізації *функціональної послуги безпеки «НИ-2»* КЗЗ ІТС забезпечує можливість однозначної ідентифікації та автентифікації обслуговуючого персоналу ІТС з використанням індивідуального ідентифікатору та паролю [2.1 (п. 2.7.6.10)].

Атрибутами доступу обслуговуючого персоналу, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами КЗЗ, є [2.1 (п. 2.7.6.10)]:

- умовний ідентифікатор в ІТС (логін);
- пароль.

Управління обліковими записами користувачами здійснюється системним адміністратором на підставі правил, наведених в [1.5].

Атрибутами доступу абонентів, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами КЗЗ, є MAC-адреса їх мережевого обладнання [2.1 (п. 2.7.6.10)].

КЗЗ ІТС забезпечує захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування [2.1 (п. 2.7.6.10)].

6.9.12. В рамках реалізації *функціональної послуги безпеки «НК-1»* КЗЗ ІТС забезпечує введення даних автентифікації користувачів здійснюється із забезпеченням неможливості їх перехоплення стороннім програмним забезпеченням [2.1 (п. 2.7.6.11)]. Для цього:

- обслуговуючий персонал попередньо ідентифікується та автентифікується засобами операційної системи робочих станцій обслуговуючого персоналу (з використанням логіну та паролю в цій операційній системі);
- після ідентифікації та автентифікації в операційній системі робочих

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Данівська Н.В.

ТОВ "АЙТІ-ІНВЕСТ" Ідентифікаційний код 37214777

станцій обслуговуючий персонал отримує термінальний доступ до відповідного мережевого обладнання для управління його налаштуваннями;

- робочі станції обслуговуючого персоналу «жорстко» співставленні з відповідним мережевим обладнанням за MAC-адресами своїх мережевих адаптерів;

- обслуговуючий персонал вводить логін та пароль доступу до відповідного мережевого обладнання.

6.9.13. В рамках реалізації *функціональної послуги безпеки «НО-1»* КЗЗ забезпечує виділення системного адміністратора, який виконує обов'язки із управління налаштуваннями апаратного та програмного забезпечення на відповідних засобах та має можливість управління обліковими записами користувачів та їх правами доступу [2.1 (п. 2.7.6.12)].

6.9.14. В рамках реалізації *функціональної послуги безпеки «НЦ-1»* КЗЗ ІТС забезпечує цілісність всього програмного та апаратного забезпечення, що входить до складу КЗЗ [2.1 (п. 2.7.6.13)]. Контроль за цілісністю КЗЗ ІТС здійснюється системним адміністратором відповідно до вимог [3.6] за умови виконання організаційно-технічних заходів [1.5].

6.9.15. В рамках реалізації *функціональної послуги безпеки «НТ-2»* КЗЗ ІТС забезпечує самотестування апаратного та програмного забезпечення, що входить до складу ІТС [2.1 (п. 2.7.6.14)]. Контроль за працездатністю та правильністю функціонування КЗЗ ІТС здійснюється системним адміністратором відповідно до вимог [3.6].

7. ВИСНОВКИ ЩОДО ВІДПОВІДНОСТІ ОБ'ЄКТА ЕКСПЕРТИЗИ ВИМОГАМ НОРМАТИВНИХ ДОКУМЕНТІВ СИСТЕМИ ТЗІ

Комплексна система захисту інформації ІТС відповідає вимогам нормативно-правових актів та нормативних документів з питань технічного захисту інформації в обсязі функцій, які викладені в документі «Технічне завдання на побудову комплексної системи захисту інформації інформаційно-телекомунікаційної системи захищеного вузлу інтернет-доступу. UA.37214777.00001.КСЗІ.ТЗ» [1.2] і забезпечує:

– конфіденційність, цілісність та доступність технологічної інформації, що забезпечує функціонування компонентів ІТС;

– розмежування доступу обслуговуючого персоналу до інформаційних ресурсів ІТС;

– ідентифікацію та автентифікацію обслуговуючого персоналу ІТС;

– доступність сервісів та ресурсів ІТС для авторизованих користувачів;

– реєстрацію дій обслуговуючого персоналу ІТС;

– захист від мережевих атак відповідно шляхом реалізації наступних функції захисту [2.1]:

- фільтрація та аналіз трафіку з використанням механізмів фільтрації спаму, контентної фільтрації, web-фільтрації, антивірусної фільтрації;

Згідно з оригіналом
Директор ТОВ «Діті - Інвест»
Данилевська Н.В.

- розмежування доступу між ІТС та зовнішніми мережами;
- інспекція мережевого трафіку та блокування пакетів або сесій, що є підозрілими, з використанням механізмів IPS / IDS;
- маскування топології і мережевих адрес ІТС від публічного перегляду;
- контроль інформаційних потоків між ІТС та інтернет-провайдерами вищого рівня з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів, в т.ч. атак типу "відмова в обслуговуванні", забезпечення реєстрації, попередження та протидії таким спробам;
- виявлення і протидія мережевим атакам і несанкціонованій мережевій активності;
- фільтрація та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;
- завершення з'єднання з вузлом, у разі атаки;
- протоколювання (реєстрація) подій, що мають відношення до безпеки;

– антивірусний захист інформації відповідно до [2.1].

8. ВИМОГИ ДО УМОВ ЕКСПЛУАТАЦІЇ ОБ'ЄКТУ ЕКСПЕРТИЗИ

Використання ІТС з комплексною системою захисту інформації можливе лише за умови дотримання вимог та положень організаційно-технічних та експлуатаційних документів, зокрема:

– технічні засоби ІТС знаходяться в контрольованій зоні, у якій забезпечується неможливість неавторизованого фізичного доступу.

– забезпечується відповідність умов експлуатації ІТС вимогам проектної документації КСЗІ [2.1];

– забезпечується відповідність технічного та програмного забезпечення ІТС, склад якого наведено у проектній та експлуатаційній документації, вимогам проектної документації [2.1];

– конфігурування комплексу засобів захисту від несанкціонованого доступу проводиться відповідно до експлуатаційної документації на нього [7];

– забезпечується відповідність конфігурування та керування компонентами, що входять до складу системного та функціонального програмного забезпечення, вимогам проектної документації КСЗІ [2.1, 7];

– забезпечується належний контроль за функціонуванням ІТС відповідно до [3.6];

– внесення змін до програмного та апаратного забезпечення ІТС повинно здійснюватись в порядку, визначеному політикою реалізації функціональних послуг безпеки «ДЗ-1», «ДВ-1» відповідно до [3.3].

Згідно з оригіналом
Директор ТОВ «Айті-Інвест»
Данилевська

Україна, Дніпропетровська обл., м.Кривий Ріг
"АЙТІ-ІНВЕСТ"
Ідентифікаційний код 37214777
Товариство з обмеженою відповідальністю

9. ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії висновку становить 5 років за умови виконання вимог розділу 8 цього висновку.

Менеджер систем інформаційної безпеки Андрій ВОЛОШИН

Начальник відділу інформаційної безпеки Юрій СЕРГІЄНКО

№ 1137/01
27.07.2020

Згідно з оригіналом
Директор ТОВ "Айті-Інвест"
Дашевська

Україна, Дніпропетровська обл., м.Кривий Ріг
"АЙТІ-ІНВЕСТ"
Ідентифікаційний код 37214777
Товариство з обмеженою відповідальністю