Прим. №1

Додаток до Атестата відповідності
№ 19211 від 17.05.2019р

Зареєстровано в Адміністрації Державної служби спеціального зв'язку та захисту інформації України
17.05.2019р. за № 19211
(дата)

Дійсний до 17.05.2024р.
(дата)

ЕКСПЕРТНИЙ ВИСНОВОК

Результати експертизи свідчать, що комплексна система захисту інформації

захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ"

(назва ІТС)

що належить **Товариству з обмеженою відповідальністю "СІТЕЛ"**

(назва організації (підприємства, установи)– власника (розпорядника),

02218, вул. Радужна, 27а

її місцезнаходження)

ВІДПОВІДАЄ

(відповідає, не відповідає)

вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі "Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Технічне завдання. Шифр – КСЗІ-ЗВ ДМІ ТОВ "СІТЕЛ".ТЗ".

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

Генеральний директор
ТОВ НДІ "Автопром"
(керівник Організатора експертизи)

(підпис) В.І. ЄФІМЕНКО

М. П.

Обл. № 26н/т

ЕКСПЕРТНИЙ ВИСНОВОК
щодо результатів експертизи комплексної системи захисту
інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ".

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, ПОЗНАЧЕНЬ ТА РОЗ'ЯСНЕНЬ

ВЗІ	–	Відповідальний за захист інформації
ДЕС	–	дизельна електростанція
Дейтаграм	–	блок інформації, надісланий як пакет мережевого рівня через передавальне середовище без попереднього встановлення з'єднання і створення віртуального каналу
ЗВ ДМІ ТОВ "СІТЕЛ"	–	захищений вузол доступу до мережі Інтернет ТОВ "СІТЕЛ"
БД	–	база даних
ПЗ	–	програмний засіб
КЗЗ	–	комплекс засобів захисту
ОС	–	операційна система
ТЗ	–	технічне завдання
ФПБ	–	функціональні послуги безпеки
SSH	–	Secure Shell – безпечна оболонка передачі даних
SNMP	–	простий протокол керування мережею
TCP	–	забезпечує надійне доправляння даних від хоста-відправника до хоста-отримувача, для цього встановлюється логічний зв'язок між хостами.
UDP	–	це один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями (датаграмами — англ. datagram) без підтвердження та гарантії доставки.
RIP	–	протокол дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію (напрямок і дальність в хопах), отримуючи її від сусідніх маршрутизаторів
ICMP	–	мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних
BGP	–	єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет
RARP	–	зворотний протокол визначення адрес (що виконує зворотне відображення адрес, тобто перетворює фізичну адресу в IP-адресу
OSPF	–	протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху
TCP/IP	–	це систематизований стек протоколів, що поділяється на чотири рівні, які корелюються з еталонною моделлю OSI. Стек протоколів TCP/IP ділиться на 4 рівні: прикладний (application), транспортний (transport), міжмережевий (internet) та рівень доступу до середовища передачі (Канальный уровень).
ARP	–	протокол визначення адреси
ARP spoofing	–	мережева атака, при якій зловмисник надсилає підроблені повідомлення протоколу ARP в локальну мережу

ЕКСПЕРТНИЙ ВИСНОВОК
щодо результатів експертизи комплексної системи захисту
інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ".

1 ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

1.1 Назва об'єкта експертизи

Повна назва – Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ".

Умовне позначення об'єкта експертизи – КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

1.2 Розробник об'єкта експертизи

Розробка КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" здійснена силами працівників Товариства з обмеженою відповідальністю "СІТЕЛ" (далі – ТОВ "СІТЕЛ"). Юридична адреса: 03150, м. Київ, вул. Антоновича, 91/14. Код ЄДРПОУ 31108855.

1.3 Вид, мета експертизи та підстави її проведення

Вид експертизи: первинна.

Державна експертиза у сфері технічного захисту інформації проведена з метою оцінки захищеності інформації, яка обробляється в ЗВ ДМІ ТОВ "СІТЕЛ", та підготовки обґрунтованих висновків щодо можливості введення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" в експлуатацію.

Оцінка захищеності інформації полягала у визначенні відповідності КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" вимогам:

– законодавчих та нормативних документів з питань технічного захисту інформації, які висуваються до даного класу інформаційно-телекомунікаційних систем, у яких обробляється відкрита інформація;

– Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Технічне завдання. Шифр – КСЗІ- ЗВ ДМІ ТОВ "СІТЕЛ".ТЗ.

Підставою для проведення експертизи є:

– Положення про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93. (у редакції наказу Адміністрації Держспецзв'язку України від 13.10.2017 № 565). Зареєстровано в Міністерстві юстиції України 16.07.2007 р. за № 820/14087;

– Рішення Експертної ради Державної служби спеціального зв'язку та захисту інформації України (Протокол від 07.12.2018р. № 35-2018);

– Договір № 1-19 від 14.01.2019 р., укладений між Товариством з обмеженою відповідальністю "СІТЕЛ" та Товариством з обмеженою відповідальністю НДІ "Автопром";

– Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Технічне завдання. Шифр – КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".ТЗ,

Затверджене Директором ТОВ "СІТЕЛ" від 22.10.2018р., Погоджене Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, від 04.11.2018р.

1.4 Замовник та Організатор експертизи

Замовником державної експертизи КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" є Товариство з обмеженою відповідальністю "СІТЕЛ" (далі – Замовник). Код ЄДРПОУ 31108855. Юридична адреса: 03150, м. Київ, вул. Антоновича, 91/14.

Організатором державної експертизи є Товариство з обмеженою відповідальністю Науково-дослідний інститут "Автопром" (далі – Організатор експертизи або Виконавець). Юридична адреса: 03150, м. Київ, вул. Тверська, 6. Код ЄДРПОУ 33102567.

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1 Загальна характеристика ЗВ ДМІ ТОВ "СІТЕЛ"

ЗВ ДМІ ТОВ "СІТЕЛ" є ІТС класу "3", в якій обробляється відкрита інформація.

КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" створена з метою забезпечення захисту інформації, що передається в ЗВ ДМІ ТОВ "СІТЕЛ", відповідно до вимог Указу Президента України №254/2017 від 30.08.2017р. "Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32".

ТОВ "СІТЕЛ" забезпечує надання послуги "Захищений доступ до мережі Інтернет" ТОВ "СІТЕЛ" в частині забезпечення передачі даних між ресурсами мережі Інтернет (загальнодоступна інформація WEB-сторінок, HTLM-документи тощо) і користувачами (абонентами).

Відповідно до «Пояснювальної записки до технічного проекту» [9] Додатку А визначено, що ТОВ "СІТЕЛ" надає абонентам послугу "Захищений доступ до мережі Інтернет", яка забезпечує:

– розподіл прав адміністратора ЗВ ДМІ ТОВ "СІТЕЛ" на керування потоками інформації від ресурсів мережі Інтернет через ЗВ ДМІ до його абонентів;

– блокування ресурсів Інтернет по IP адресі за зверненням від користувача (абонента);

– надавання користувачам переліку сеансів зв`язку за вказаний період;

– аналіз потоків інформації за допомогою сервера аналізу загроз;

– у випадку DDoS атаки блокування скомпрометованих IP адрес користувача.

ЗВ ДМІ ТОВ "СІТЕЛ" має власну розгалужену мережу з потужними вузлами доступу до мережі Інтернет (територіально розподілені майданчики Провайдера (вузли) –детальніше п 2.2.2.1), що дозволяють надавати послуги по території України.

ЗВ ДМІ ТОВ "СІТЕЛ" представляє собою організаційно-технічну систему, що об'єднує обчислювальну систему (технічне та програмне забезпечення ЗВ ДМІ ТОВ "СІТЕЛ"), фізичне середовище, персонал і оброблювану інформацію.

2.2 Склад обчислювальної системи ЗВ ДМІ ТОВ "СІТЕЛ"

У документах [5], [6], [9], [32] Додатку А визначений такий склад ЗВ ДМІ ТОВ "СІТЕЛ" :

– адміністративного сегменту;

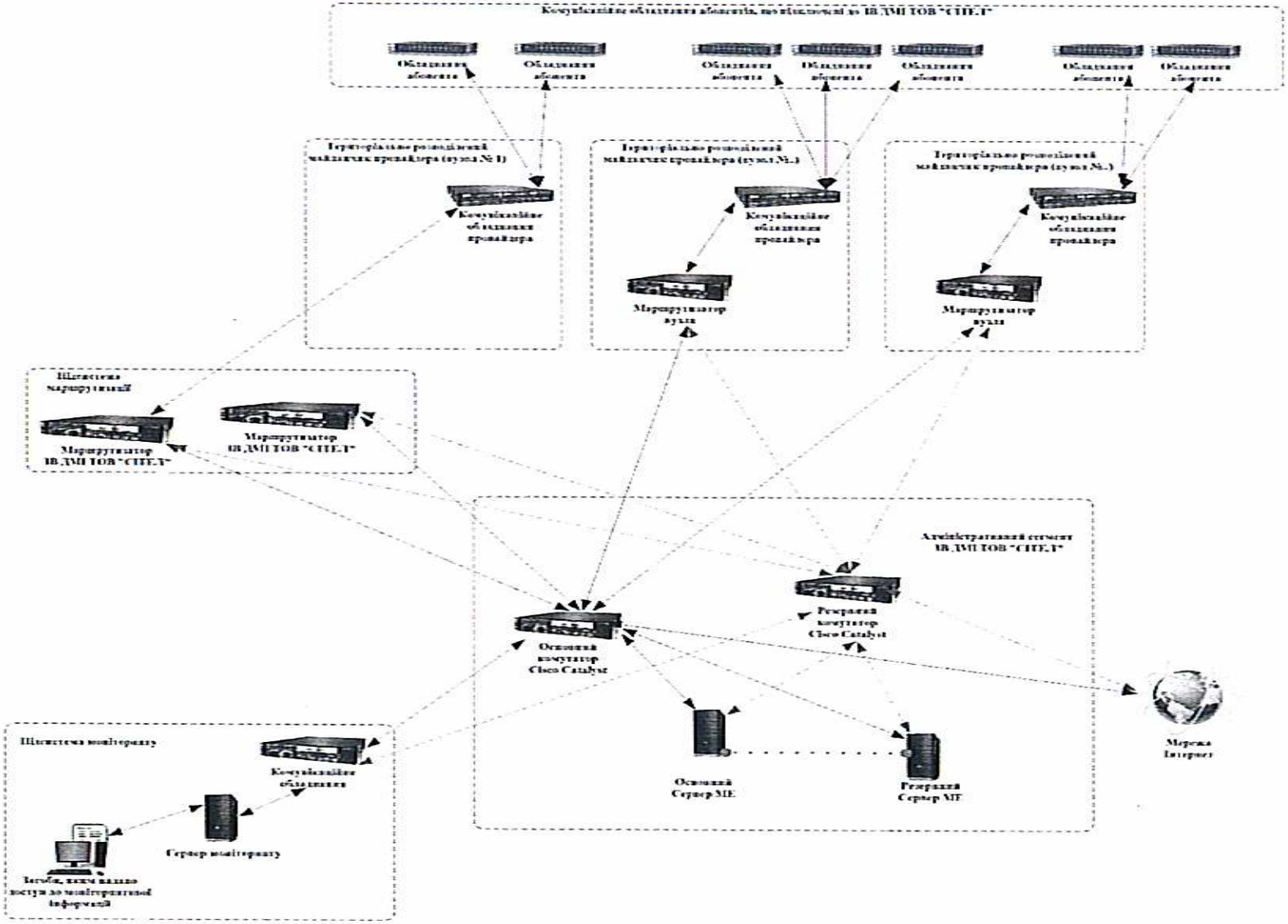
– підсистеми моніторингу.

– територіально розподілених майданчиків провайдера (вузлів);

– підсистеми маршрутизації.

Структура ЗВ ДМІ ТОВ "СІТЕЛ" наведена на малюнку 1.1.

ЕКСПЕРТНИЙ ВИСНОВОК
щодо результатів експертизи комплексної системи захисту
інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ".



Малюнок 2.1 – Структура мережі ЗВ ДМІ ТОВ "СІТЕЛ"

2.2.1 Технічне обладнання ЗВ ДМІ ТОВ "СІТЕЛ"

2.2.1.1 У документах [9], [32] Додатку А визначено такий склад технічного обладнання ЗВ ДМІ ТОВ "СІТЕЛ" адміністративного сегменту:

– основний та резервний сервер міжмережевого екрану (далі – Сервер МЕ): DELL PowerEdge R210 II;

– міжмережеве обладнання адміністративного сегменту: Cisco Catalyst WS C3560G-24TS-S.

2.2.1.2 У документах [9], [32] Додатку А визначено такий склад технічного обладнання ЗВ ДМІ ТОВ "СІТЕЛ" підсистеми моніторингу входить:

– сервер моніторингу (далі – Сервер моніторингу): S/N: AZRY0240079;

– комунікаційне обладнання ЗВ ДМІ ТОВ "СІТЕЛ";

– засоби, яким надано доступ до моніторингової інформації.

2.2.1.3 Міжмережеве обладнання ЗВ ДМІ ТОВ "СІТЕЛ", яке розташоване на територіально розподілених майданчиках провайдера (вузлах), визначене в "Переліку територіально розподілених майданчиків, включених до ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.ПІ.02" ([6] Додатку А).

2.2.1.4 Підсистеми маршрутизації розгорнуті для забезпечення потреб окремих абонентів, до яких входять кластери маршрутизаторів ЗВ ДМІ ТОВ "СІТЕЛ". Підсистеми маршрутизації розміщуються в окремо відділених приміщеннях, що знаходяться під охороною. Склад Підсистеми маршрутизації визначено в документі "Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Формуляр. UA.31108855.КСЗІ.00001.ФО" ([32] Додатку А).

2.2.1.5 У документі [9] Додатку А визначено, що Сервер МЕ забезпечує:

– адміністрування компонентів ЗВ ДМІ ТОВ "СІТЕЛ";

– фільтрацію та аналіз трафіку на рівнях L3- L7 моделі OSI;

– розмежовування доступу між серверами ЗВ ДМІ ТОВ "СІТЕЛ" та зовнішніми мережами;

– інспекцію (аналіз) мережевого трафіку та блокування пакетів або сесій, що є підозрілими;

– маскування топології ЗВ ДМІ ТОВ "СІТЕЛ" і мережевих адрес від публічного перегляду;

– проходження між сегментами мережі лише дозволених інформаційних потоків згідно визначених протоколів;

– реєстрацію подій, пов'язаних з отриманням адміністраторами ЗВ ДМІ ТОВ "СІТЕЛ" та безпеки доступу на керування засобами мережевого захисту та міжмережевого екранування, та дій щодо їх конфігурування;

– збереження конфігураційних файлів та системного програмного забезпечення (далі –ПЗ) засобів мережевого захисту та міжмережевого екранування з метою їх подальшого швидкого відновлення в разі збоїв.

Фільтрація трафіку здійснюється завдяки програмному фаерволу ЗВ ДМІ ТОВ "СІТЕЛ" на основі набору попередньо сконфігурованих правил та реалізації на прикладному рівні розподілу трафіку між мережевими пристроями та фізичного поділу між локальною мережею і мережі з ізолюванням трафіку один від одного за допомогою протоколу 802.1Q та технології VLAN.

Протокол IEEE 802.1Q або VLAN Tagging — мережевий стандарт, який використовується, для сумісного використання фізичної мережі Ethernet багатьма логічними (віртуальними) мережами. IEEE 802.1Q визначає віртуальну мережу (virtual LAN або VLAN) відповідно до моделі комутації пакетів на рівні MAC та протоколу IEEE 802.1D (Протокол забезпечує обмін даними між об'єктами мережі, підключеними до різних VLAN'ів, крізь комутатори мережевого рівня або маршрутизатори).

VLAN є групою хостів з загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі.

2.2.1.6 У документі [9] Додатку А визначено, що міжмережеве обладнання адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ" - основний та резервний центральний комутатор Cisco Catalyst WS C3560G-24TS-S (далі комутатори Cisco), які забезпечують:

– ідентифікацію внутрішнього користувача ЗВ ДМІ ТОВ "СІТЕЛ" на основі політики авторизації (внутрішня IP-адреса);

– ідентифікацію процесів абонентів ЗВ ДМІ ТОВ "СІТЕЛ" на рівні IP-адреси, MAC-адреси відправника/одержувача;

– виконання перевірки стану обладнання та маршрутизації;

– реалізацію динамічного контролю ARP DAI (функція захисту від ARP spoofing атак. За допомогою ARP spoofing зловмисник посилає підроблене повідомлення на локальну мережу);

– контроль доступу до MAC-адреси.

2.2.1.7 У документі [9] Додатку А визначено, що сервер моніторингу забезпечує:

– відображення постійно зміновальної інформації щодо стану мережі ЗВ ДМІ ТОВ "СІТЕЛ";

– зберігання архівних копій критичної для ЗВ ДМІ ТОВ "СІТЕЛ" інформації а саме:

- параметри конфігурації мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ";
- параметри конфігурації сервісів безпеки міжмережевого екрану;
- журнали реєстрації подій серверів, мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ" та сервісів безпеки міжмережевого екрану.

2.2.1.8 У документі [9] Додатку А визначено, що засоби, яким надано доступ до моніторингової інформації – це автоматизовані робочі місця, смартфони та планшети робітників ЗВ ДМІ ТОВ "СІТЕЛ", яким шляхом налаштування ПЗ моніторингу надано доступ до постійно зміцнювальною моніторингової інформації щодо стану мережі ЗВ ДМІ ТОВ "СІТЕЛ" (детальніше п. 2.2.2.5).

2.2.1.9 Комунікаційне обладнання підсистеми моніторингу забезпечує зв'язок з адміністративним сегментом ЗВ ДМІ ТОВ "СІТЕЛ".

2.2.1.10 У документі [9] Додатку А визначено, що до міжмережевого обладнання, яке безпосередньо розташоване на територіально розподілених майданчиках провайдера (вузлах), належить комутаційне обладнання провайдера та маршрутизатори майданчика для підключення до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ". Комутаційне обладнання провайдера та маршрутизатори майданчика наведені в "Переліку територіально розподілених майданчиків, включених до ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.ПІ.02" ([6] Додатку А).

2.2.1.11 У документі [9] Додатку А визначено, що маршрутизатори ЗВ ДМІ ТОВ "СІТЕЛ" забезпечують:

– ідентифікацію користувача на основі політики авторизації;

– самотестування при старті;

– реєстрацію подій;

– буферизацію з центральним вузлом системи, який з'єднує всі інші блоки один з одним;

– перевірку основних заголовків пакетів, що приходять на маршрутизатор (блок-пошук);

– налаштування пошуку маршруту.

2.2.1.12 "Перелік територіально розподілених майданчиків, включених до ЗВ ДМІ ТОВ "СІТЕЛ"" ([12] Додатку А), затверджено директором ТОВ "СІТЕЛ".

Відповідно до документу [9] та [24] Додатку А у приміщеннях територіально розподілених майданчиків Провайдера забезпечується:

– розміщення міжмережевого обладнання, яке безпосередньо розташоване на територіально розподілених майданчиках провайдера (вузлах);

– безперебійне стабільне електроживлення міжмережевого обладнання, яке безпосередньо розташоване на територіально розподілених майданчиках провайдера (вузлах);

– стабільні кліматичні умови;

– охорона міжмережевого обладнання, яке безпосередньо розташоване на територіально розподілених майданчиках провайдера (вузлах).

2.2.1.13 Комунікаційне обладнання абонентів, що підключені до ЗВ ДМІ ТОВ "СІТЕЛ" – це комутатори та маршрутизатори абонентів (є власністю абонентів), які відповідно до договорених відносинам підключені до територіально розподілених майданчиків провайдера (вузлів)ЗВ ДМІ ТОВ "СІТЕЛ".

2.2.1.14 У разі відмов електроживлення на адміністративному сегменті надається резервне електроживлення від джерел безперебійного живлення, які забезпечуються шляхом:

– автоматичного включення резерву;

– підключення до дизельної генеруючої установки.

2.2.2 Програмне забезпечення ЗВ ДМІ ТОВ "СІТЕЛ"

2.2.2.1 У документах [9] та [32] Додатку А визначено такий склад програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ" складається з:

– системного програмного забезпечення (далі – ОС сервера):

- ОС серверу МЕ – CentOS Linux v.7 – RELEASE;
- ОС серверу моніторингу – FreeBSD 9.2-STABLE;

– функціонального програмного забезпечення:

- ПЗ міжмережевого екрану – набір попередньо конфігурованих правил щодо фільтрації трафіку абонентів на рівні ядра CentOS Linux v.7 – RELEASE;
- ПЗ md5sum - дозволяє обчислювати значення хеш-сум (контрольних сум) контролюючого файлу, що виконується на рівні ядра CentOS Linux v.7– RELEASE;
- ПЗ Nagios 4.4 (далі – ПЗ моніторингу);
- програмне забезпечення антивірусного захисту - ESET Gateway Security для Linux/BSD/Solaris версії 4.5.

2.2.2.2 ОС серверів забезпечує функціонування ПЗ ЗВ ДМІ ТОВ "СІТЕЛ".

2.2.2.3 У документі [9] Додатку А визначено, що ПЗ міжмережевого екрану забезпечує фільтрацію трафіку абонентів на основі набору попередньо сконфігурованих правил. Фільтрація трафіку виконується на рівні ядра Linux. Правила фільтрації трафіку налаштовано відповідно до «Інструкції з адміністрування системи» ([12] Додатку А).

2.2.2.4 У документі [9] Додатку А визначено, що ПЗ md5sum (далі – ПЗ забезпечення цілісності) – це додаткова програма, що дозволяє обчислювати значення хеш-сум (контрольних сум) файлів ПЗ міжмережевого екрану за алгоритмом MD5 та сигналізує у разі виявлення порушень. ПЗ забезпечення цілісності виконується на рівні ядра CentOS Linux v.7– RELEASE. ПЗ забезпечення цілісності налаштовано відповідно до «Інструкції з адміністрування системи» ([12] Додатку А).

2.2.2.5 У документі [9] Додатку А визначено, що ПЗ моніторингу забезпечує:

– моніторинг мережевих служб;

– моніторинг стану хостів-вузлів (завантаження процесора, використання диска, системні логи) у мережевих операційних систем;

– встановлення ієрархії хостів-вузлів мережі за допомогою "батьківських" хостів-вузлів, та виявлення і розрізнення хостів-вузлів, які вийшли з ладу, і ті, які недоступні;

– відправку оповіщень у разі виникнення проблем зі службою або хостом на засоби, яким надано доступ до моніторингової інформації (за допомогою пошти, пейджера, смс);

– налаштування параметрів автоматичної ротації лог-файлів;

2.2.2.6 У документі [9] Додатку А визначено, що програмне забезпечення антивірусного захисту забезпечує:

– запобігання проникненню комп'ютерних вірусів;

– оперативне виявлення та знешкодження комп'ютерних вірусів у випадку їхнього проникнення.

2.3 Середовище користувачів ЗВ ДМІ ТОВ "СІТЕЛ"

2.3.1 За рівнем повноважень щодо доступу до інформації та характеру робіт, що виконуються в процесі функціонування ЗВ ДМІ ТОВ "СІТЕЛ", особи, які мають доступ до ЗВ ДМІ ТОВ "СІТЕЛ", поділяються на такі категорії:

– звичайні користувачі – абоненти, яким надано право доступу тільки до загальнодоступної інформації WEB-ресурсів;

– користувачі, які забезпечують функціонування ЗВ ДМІ ТОВ "СІТЕЛ" та здійснюють адміністрування операційної системи (ОС) та комплексу засобів захисту (КЗЗ):

- оператори мережевого обладнання;
- системні адміністратори;

- адміністратори безпеки.

2.3.2 У документах [9] та [13] Додатку А визначено, що Оператори мережевого обладнання виконують такі функції:

– налаштування параметрів міжмережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ", з метою забезпечення надання послуг абонентам доступу до мережі Інтернет;

– налаштування параметрів правил фільтрації міжмережевого екрану;

– введення/виведення даних щодо абонентів ЗВ ДМІ ТОВ "СІТЕЛ".

2.2.1 У документах [9] та [12] Додатку А визначено, що «Адміністратор безпеки» виконує такі функції:

– здійснює загальний контроль за станом безпеки в ЗВ ДМІ ТОВ "СІТЕЛ";

– контролює відповідність налаштувань програмних та технічних засобів прийнятій політиці безпеки;

– реєстрація нових користувачів та видалення старих користувачів в ЗВ ДМІ ТОВ "СІТЕЛ";

– призначення атрибутів доступу користувачів та об'єктів захисту;

– надання користувачам прав доступу до об'єктів захисту;

– перегляд аудиту подій щодо автентифікації і авторизації користувачів ЗВ ДМІ ТОВ "СІТЕЛ", доступу до об'єктів захисту, а також оброблення та аналіз зареєстрованої інформації про критичні з погляду безпеки події;

– архівація технологічної інформації КЗЗ.

2.2.2 У документах [9] та [12] Додатку А визначено, що «Системний адміністратор» виконує такі функції:

– забезпечує працездатність компонентів ЗВ ДМІ ТОВ "СІТЕЛ" в цілому;

– проводить налаштування апаратного і програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ";

– технічне обслуговування апаратного і програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ";

– резервне копіюванню налаштувань ЗВ ДМІ ТОВ "СІТЕЛ" та відновлення працездатності ЗВ ДМІ ТОВ "СІТЕЛ";

– здійснює аналіз журналів реєстрації подій;

– моніторинг стану ЗВ ДМІ ТОВ "СІТЕЛ".

2.3.3 Абоненти одержують доступ до WEB-сторінок у відповідності до чинних у мережі Інтернет правил та регламенту. Вимоги до абонентів, яким надається право доступу до загальнодоступної інформації WEB-ресурсів, не висуваються.

2.3.4 Налаштування кожного апаратно–програмного засобу захисту КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується адміністраторами ЗВ ДМІ ТОВ "СІТЕЛ", в рамках своїх повноважень при безпосередньому доступі до засобу захисту.

2.4 Фізичне середовище

2.4.1 Розміщення обчислювальної системи компонентів ЗВ ДМІ ТОВ "СІТЕЛ" виконано, виходячи з:

– локалізації технічних засобів у приміщенні, фізичний доступ до якого є обмеженим;

– технічних характеристик обладнання та вимог щодо його встановлення і умов експлуатації, визначених їх виробником.

2.4.2 Технічні засоби адміністративного сегмента ЗВ ДМІ ТОВ "СІТЕЛ" у складі: Серверів МЕ та міжмережевого обладнання адміністративного сегмента розміщуються за адресою: 02218, вул. Радужна, 27а.

2.4.3 Технічні засоби підсистеми моніторингу розміщуються за адресою: Киев, вул. Барбюса 37/1, оф. 500.

2.4.4 Перелік територіально розподілених майданчиків Провайдера, включених до ЗВ ДМІ ТОВ "СІТЕЛ" затверджено Наказом директором ТОВ "СІТЕЛ" від 20.02.2019р.

2.4.5 У приміщеннях територіально розподілених майданчиків Провайдера (вузлів) забезпечується:

– розміщення міжмережевого обладнання майданчика Провайдера;

– безперебійне електроживлення обладнання майданчика;

– стабільні кліматичні умови;

– охорона міжмережевого обладнання майданчика.

2.4.6 Вищезазначені заходи щодо обмеження та контролю доступу унеможливлюють перебування сторонніх осіб в приміщеннях, де розміщуються компоненти ЗВ ДМІ ТОВ "СІТЕЛ".

2.5 Інформаційне середовище ЗВ ДМІ ТОВ "СІТЕЛ"

2.5.1 Відповідно до вимог Указу Президента України №254/2017 від 30.08.2017 р. "Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного

в дію Указом Президента України від 13 лютого 2017 року № 32" висуваються вимоги до створення КСЗІ в ІТС Інтернет-провайдерів із надання абонентам послуг доступу до мережі Інтернет.

2.5.2 Згідно з "Переліком інформації, що підлягає захисту під час її обробки в інформаційно-телекомунікаційній системі ТОВ "ЗВ ДМІ ТОВ "СІТЕЛ", який затверджений директором ТОВ "СІТЕЛ" ([2] Додатку А), в ЗВ ДМІ ТОВ "СІТЕЛ" обробляється відкрита інформація.

2.5.3 У документах [2], [5], [8], [9] Додатку А визначено, що інформація, яка обробляється в ЗВ ДМІ ТОВ "СІТЕЛ", за функціональною ознакою поділяється на:

– транзитну інформацію мережного обладнання ЗВ ДМІ ТОВ "СІТЕЛ";

– технологічну інформацію:

- внутрішня IP-адреса;
- логін та пароль доступу до мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ";
- логін та пароль доступу до ОС Серверів ЗВ ДМІ ТОВ "СІТЕЛ";
- параметри конфігурації серверів;
- параметри конфігурації мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ";
- параметри конфігурації сервісів безпеки міжмережевого екрану;
- журнали реєстрації подій.

2.5.4 До інформації, яка обробляється в ЗВ ДМІ ТОВ "СІТЕЛ", висуваються вимоги із забезпечення конфіденційності, цілісності та доступності.

2.6 Технологія обробки інформації в ЗВ ДМІ ТОВ "СІТЕЛ"

Відповідно до «Пояснювальної записки до технічного проекту» [9] Додатку А визначено, така технологія обробки інформації в ІТС ЗВ ДМІ ТОВ "СІТЕЛ":

– отримання ІТС ЗВ ДМІ ТОВ "СІТЕЛ" доступу до глобальної мережі Інтернет;

– адміністрування мережевого обладнання ІТС ЗВ ДМІ ТОВ "СІТЕЛ";

– ведення, опрацювання та зберігання інформації щодо абонентів ЗВ ДМІ ТОВ "СІТЕЛ";

– резервне копіювання.

2.6.1 Технологія отримання ІТС ЗВ ДМІ ТОВ "СІТЕЛ" доступу до глобальної мережі Інтернет

Згідно з умовами Договору № ВК-4400-01/12 від 30.01.2012р. ТОВ "Дабл-Ю Нет Україна"1 (далі – Оператор) надає ТОВ "СІТЕЛ" (далі – Провайдер) послуги доступу до

1 Код ЄДРПОУ: 37002401, Юридична адреса: 01103, м. Київ, вул.Кіквідзе,буд.14 в,оф.4. Тел.: +380 44 590 08 00

мережі Інтернет, організовує оптоволоконні лінії зв'язку, цифрові канали місцевого продовження (транспортні канали).

Принцип мережі глобальної мережі Інтернет наступний:

– абоненти підключаються до мережі Інтернет через регіональних провайдерів;

– регіональний провайдер, підключається до провайдеру національного масштабу, що має вузли в різних містах країни;

– мережі національних провайдерів об'єднуються в мережі транснаціональних провайдерів або провайдерів першого рівня. Об'єднані мережі провайдерів першого рівня становлять глобальну мережу Internet.

Відповідно до принципу побудови мережі Інтернет:

– ТОВ "СІТЕЛ" є регіональним провайдером;

– ТОВ "Дабл-Ю Нет Україна" є провайдером національного масштабу.

ТОВ "Дабл-Ю Нет Україна" організовує транспортні канали та підключає порти мережі Провайдера до портів власної телекомунікаційної мережі. Порядок транспортних каналів, підключення та експлуатації кінцевого обладнання наведений в Договорі № ВК-4400-01/12 від 30.01.2012р.

Користувачі ЗВ ДМІ ТОВ "СІТЕЛ" з роллю "адміністратор безпеки" та "системний адміністратор" здійснюють організацію підключення (відключення) до транспортних каналів провайдера національного масштабу відповідно до Порядку, що зазначений у розділі 5 документу [22] Додатку А.

2.6.2 Технологія адміністрування мережевого обладнання ІТС ЗВ ДМІ ТОВ "СІТЕЛ"

Для забезпечення трансляції транзитної інформації абонентів ЗВ ДМІ ТОВ "СІТЕЛ" оператором мережевого обладнання здійснюється адміністрування мережевого обладнання, яке розташоване на територіально розподілених майданчиках Провайдера з використанням TCP/IP-моделі передачі даних на:

– транспортному рівні (transport) – основне завдання якого – це надання транспортних послуг прикладним процесам. Основними протоколами транспортного рівня TCP/IP є протокол керування передавання TCP та протокол користувальницьких дейтаграм UDP. Протокол UDP доставляє дейтаграми без установлення з'єднання. При цьому він не гарантує їхнього доставляння. Протокол TCP забезпечує надійне доставляння байтових потоків (сегментів) із попереднім встановленням транспортного дуплексного з'єднання

(віртуального каналу) між модулями TCP мережевих комп'ютерів. Кожний прикладний процес взаємодіє з модулем транспортного рівня TCP або UDP через окремий порт, що дозволяє при взаємодії систем однозначно ідентифікувати прикладні процеси;

– міжмережевому рівні (internet) – основне завдання якого - це маршрутизація пакетів даних між різнотипними комп'ютерними мережами. Для розв'язання цього завдання протокол IP підтримує IP-адресацію мереж та вузлів, використовує таблицю маршрутизації пакетів, виконує, за необхідності, фрагментацію та дефрагментацію цих пакетів. Основним протоколом мережного рівня технології TCP/IP є міжмережевий протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів тощо. Функціонування мережевого рівня також забезпечує низка протоколів динамічної маршрутизації RIP, OSPF, які динамічно формують маршрути таблиці маршрутизації та BGP (Border Gateway Protocol).

Для об'єднання компонентів ІТС ЗВ ДМІ ТОВ "СІТЕЛ" в локальну обчислювальну мережу ІТС ЗВ ДМІ ТОВ "СІТЕЛ" використовується внутрішня IP – адреса, або фізичне з'єднання на рівні кабельного з'єднання. Внутрішня IP - адреса – це додатковий ідентифікатор технічного засобу ІТС ЗВ ДМІ ТОВ "СІТЕЛ". Внутрішня IP – адреса не використовується (маршрутизується) в мережі Інтернет, на неї не можливо відправити трафік з Інтернету, вона працює лише в мережі ІТС ЗВ ДМІ ТОВ "СІТЕЛ". Налаштування внутрішньої IP – адреси забезпечується адміністратором безпеки (відповідно до документу [12] Додатку А).

2.6.3 Технологія ведення, опрацювання та збереження інформації ЗВ ДМІ ТОВ "СІТЕЛ"

2.6.2.1 На Сервері МЕ здійснюється фільтрація трафіку завдяки програмному фаерволу ЗВ ДМІ ТОВ "СІТЕЛ" на основі набору попередньо сконфігурованих правил у частині:

– пакетного фільтру, що контролюють проходження трафіку на основі інформації, що міститься в заголовку пакетів. При аналізі заголовка мережевого пакету використовуються такі параметри:

- IP-адреси джерела і одержувача;
- тип транспортного протоколу;
- поля службових заголовків протоколів мережевого і транспортного рівнів;

▪ порт джерела і одержувача.

– шлюзу сеансового рівня, що виключає пряму взаємодію зовнішніх хостів з вузлом, розташованим в локальній мережі, виступаючи в якості посередника, який реагує на всі вхідні пакети і перевіряє їх допустимість на підставі поточної фази з'єднання. Процес взаємодії такий: при запиті на встановлення з'єднання, в спеціальну таблицю поміщається відповідна інформація (адреси відправника і одержувача, використовувані протоколи мережевого і транспортного рівня, стан з'єднання і т. д.), у разі, якщо з'єднання встановлено, пакети, що передаються в рамках даної сесії, будуть просто копіюватися в локальну мережу без додаткової фільтрації. При завершенні сеансу зв'язку, відомості про сеанс нього видаляються з даної таблиці. Шлюз сеансового рівня запобігає можливість реалізації DoS-атаки, властивою пакетним фільтрам.

2.6.2.2 На Сервері моніторингу здійснюється відображення на засоби ЗВ ДМІ ТОВ "СІТЕЛ", які мають доступ до ПЗ моніторингу, постійно змінювальної інформації щодо стану мережі ЗВ ДМІ ТОВ "СІТЕЛ".

2.6.2.3 Користувачем з роллю "Оператор мережевого обладнання" на Сервері МЕ здійснюється редагування налаштувань правил фільтрації трафіку міжмережевого екрану та мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ" (відповідно до документу [13] Додатку А).

2.6.2.4 На сервері МЕ користувач з роллю "Оператор мережевого обладнання" здійснює підключення та вилучення абонентів ЗВ ДМІ ТОВ "СІТЕЛ" відповідно до Порядку, що зазначений у розділі 5 документу [13] Додатку А.

2.6.4 Технологія резервного копіювання

В ЗВ ДМІ ТОВ "СІТЕЛ" реалізована ручна процедура резервного копіювання на резервний Сервер МЕ. Правила резервування наведені в документі "Технологічна інструкція з резервування та відновлення інформації В ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.И5" ([23] Додатку А).

Відповідно до документів [9], [8] та [23] Додатку А резервному копіюванню в ЗВ ДМІ ТОВ "СІТЕЛ" підлягають:

– параметри конфігурації серверів:

– параметри конфігурації мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ";

– параметри конфігурації сервісів безпеки міжмережевого екрану;

– журнали реєстрації подій серверів, мережевого обладнання ЗВ ДМІ ТОВ "СІТЕЛ" та сервісів безпеки міжмережевого екрану.

2.7 Склад КСЗІ, що подається на експертне оцінювання

2.7.1 Завдання захисту, вирішення яких забезпечується об'єктом експертизи

Об'єктом експертизи вирішуються такі завдання захисту інформації в ЗВ ДМІ ТОВ "СІТЕЛ":

– реалізація політики безпеки інформації, заданої в ЗВ ДМІ ТОВ "СІТЕЛ";

– ідентифікація та автентифікація користувачів/процесів у ході надання їм доступу до функцій ЗВ ДМІ ТОВ "СІТЕЛ";

– забезпечення конфіденційності, цілісності інформації, що обробляється у ЗВ ДМІ ТОВ "СІТЕЛ";

– розмежування доступу користувачів/процесів до ресурсів ЗВ ДМІ ТОВ "СІТЕЛ";

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

– ефективне попередження, своєчасне виявлення та знешкодження загроз для ресурсів ЗВ ДМІ ТОВ "СІТЕЛ", причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;

– керування засобами захисту інформації, у тому числі і сервісами безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", з боку осіб, які відповідають за забезпечення безпеки інформації ЗВ ДМІ ТОВ "СІТЕЛ";

– створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення функціонування ЗВ ДМІ ТОВ "СІТЕЛ";

– реєстрація, збір, зберігання, обробка даних про події у ЗВ ДМІ ТОВ "СІТЕЛ", які мають відношення до безпеки інформації;

– забезпечення доступності ресурсів ЗВ ДМІ ТОВ "СІТЕЛ" для її користувачів;

– забезпечення працездатності та оперативного відновлення ЗВ ДМІ ТОВ "СІТЕЛ" при виникненні позаштатних чи аварійних ситуацій;

– забезпечення захисту обчислювальних ресурсів та компонентів ЗВ ДМІ ТОВ "СІТЕЛ" від атак та несанкціонованого доступу з боку мережі Інтернет (в тому числі унеможливлення попадання шкідливого ПЗ до ЗВ ДМІ ТОВ "СІТЕЛ");

– забезпечення розгортання додаткових територіально розподілених майданчиків Провайдера.

КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" - це сукупність організаційних заходів та технічних заходів захисту, програмних та програмно-апаратних засобів, які забезпечують захист інформації у відповідності до нормативно–правових документів у галузі захисту інформації та які дозволяют обробляти у ЗВ ДМІ ТОВ "СІТЕЛ" інформацію відповідно до її призначення та ступеню обмеження доступу.

2.7.2 Організаційні заходи захисту

2.7.2.1 Організаційні заходи захисту інформації – це комплекс адміністративних та обмежувальних заходів, спрямованих на вирішення задач захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів забезпечення інформаційної діяльності та засобів забезпечення технічного захисту інформації.

2.7.2.2 Основні організаційні заходи такі:

– призначено Відповідального за захист інформації (далі – ВЗІ), якому надано повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації;

– визначено політику безпеки інформації у ЗВ ДМІ ТОВ "СІТЕЛ";

– розроблено й впроваджено План захисту інформації у ЗВ ДМІ ТОВ "СІТЕЛ"

– реалізовані положення політики безпеки;

– розроблено порядок реєстрації у ЗВ ДМІ ТОВ "СІТЕЛ" всіх користувачів і їх дій з об'єктами захисту;

– регламентовано доступ користувачів різних категорій до об'єктів захисту ЗВ ДМІ ТОВ "СІТЕЛ";

– розроблено порядок проведення відновлювальних робіт і забезпечення безперервного функціонування ЗВ ДМІ ТОВ "СІТЕЛ";

– розроблено порядок проведення модернізації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

2.7.2.3 Фізична цілісність критичних апаратних компонентів забезпечується організаційними заходами й застосуванням пломб (наліпок, печаток та ін.) на блоках і пристроях засобів обчислювальної техніки. Повсякденний контроль цілісності й відповідності пломб, наліпок компонентів здійснюється представниками ТОВ "СІТЕЛ". Періодичний контроль критичних апаратних компонентів здійснюється ВЗІ.

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

– системи нормативно-правового забезпечення робіт із захисту інформації у ЗВ ДМІ ТОВ "СІТЕЛ";

– процедур доведення до персоналу ЗВ ДМІ ТОВ "СІТЕЛ" основних положень політики безпеки інформації, їхнього навчання й підвищення кваліфікації з питань безпеки інформації;

– системи контролю своєчасності, ефективності й повноти реалізації у ЗВ ДМІ ТОВ "СІТЕЛ" рішень із захисту інформації, дотримання персоналом положень політики безпеки.

2.7.2.5 На технічному рівні для блокування загроз НСД до інформаційних ресурсів ЗВ ДМІ ТОВ "СІТЕЛ" застосовуються КЗЗ та сервісів безпеки у складі обчислювальної системи ЗВ ДМІ ТОВ "СІТЕЛ".

2.7.2.6 Політикою безпеки ЗВ ДМІ ТОВ "СІТЕЛ" визначено адміністративний принцип керування доступом до всіх об'єктів захисту.

2.7.2.7 У обчислювальній системі ЗВ ДМІ ТОВ "СІТЕЛ" адміністратор безпеки є спеціально авторизованим користувачем, якому надані повноваження щодо керування потоками інформації від захищених об'єктів до користувачів.

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

– ВЗІ здійснює контроль доступу користувачів до об'єктів захисту;

– фізичний доступ у приміщення, де розміщуються компоненти ЗВ ДМІ ТОВ "СІТЕЛ", здійснюється згідно списку та контролюється співробітниками охорони;

– склад обчислювальної системи ЗВ ДМІ ТОВ "СІТЕЛ" визначено у Формулярі і його незмінність контролюється адміністратором безпеки;

– перелік територіально розподілених майданчиків затверджений Наказом директора ТОВ "СІТЕЛ";

– у складі програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ" відсутні програми, які не призначені для вирішення функціональних завдань;

– користувачам заборонено встановлювати будь-яке програмне забезпечення на компоненти ЗВ ДМІ ТОВ "СІТЕЛ".

2.7.2.9 Адміністратор безпеки виконує такі функції:

– організація та контроль якісного виконання організаційно-технічних заходів з захисту інформації в ЗВ ДМІ ТОВ "СІТЕЛ";

– адміністрування облікових записів користувачів;

– керування атрибутами доступу користувачів ЗВ ДМІ ТОВ "СІТЕЛ", які використовуються для доступу до ресурсів;

– керування журналами аудиту подій в ЗВ ДМІ ТОВ "СІТЕЛ";

– відстеження подій безпеки та реагування на інциденти безпеки;

– налаштування параметрів безпеки КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– контроль параметрів безпеки КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– контроль функціонування КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– організація та здійснення заходів з резервного копіювання та відновлення технологічної інформації КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

2.7.2.10 В ЗВ ДМІ ТОВ "СІТЕЛ" користувач/процес, який намагається одержати доступ до ресурсів, виконує в обов'язковому порядку процедуру входу (реєстрації) у систему. При вході в систему здійснюється ідентифікація (розпізнавання) і автентифікація (підтвердження автентичності) користувача (суб'єкта).

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

2.7.3 Технічні заходи захисту

Технічні заходи захисту у рамках створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", такі:

– перевірка працездатності технічних засобів ЗВ ДМІ ТОВ "СІТЕЛ";

– своєчасне резервування критичних ресурсів ЗВ ДМІ ТОВ "СІТЕЛ";

– використання резервного електроживлення технічних засобів системи.

2.7.4 Програмні засоби захисту

2.7.4.1 В документі [9] Додатку А визначено, що до складу програмних засобів захисту ЗВ ДМІ ТОВ "СІТЕЛ" входять:

– ПЗ ЗВ ДМІ ТОВ "СІТЕЛ":

- сервіси безпеки ОС серверів:
  - ОС серверу МЕ – CentOS Linux v.7– RELEASE;
  - ОС серверу моніторингу – FreeBSD 9.2-STABLE;
- ПЗ міжмережевого екрану – набір попередньо конфігурованих правил щодо фільтрації трафіку абонентів на рівні ядра CentOS Linux v.7 – RELEASE;

▪ ПЗ md5sum - дозволяє обчислювати значення хеш-сум (контрольних сум) контролюючого файлу (ПЗ міжмережевого екрану), що виконується на рівні ядра CentOS Linux v.7– RELEASE;

▪ засоби антивірусного захисту (далі – ПЗ антивірусного захисту) – ESET Gateway Security для Linux/BSD/Solaris версії 4.5;

– ОС апаратно-програмних засобів (далі – АПЗ) ЗВ ДМІ ТОВ "СІТЕЛ":

▪ ОС Cisco Catalyst;

▪ ОС мережевого обладнання майданчикіє провайдера.

2.7.4.2 Сервіси безпеки ОС серверів забезпечують виконання таких функцій захисту:

– ідентифікація та автентифікація внутрішнього користувача ОС на основі внутрішньої IP- адреси, логіну та паролю;

– надання достовірного каналу для введення атрибутів користувачів ОС;

– підтримка множини локальних ролей адміністраторів та користувачів на рівні ОС;

– фільтрація мережевих з'єднань;

– захист від несанкціонованого доступу до об'єктів захисту, що зберігаються у файловій системі ОС серверу;

– забезпечення безперервності функціонування ОС;

– забезпечення цілісності компонентів;

– автоматичне відновлення ОС після збоїв;

– відновлення стану ОС на певний момент часу;

– ведення журналів аудиту.

2.7.4.3 Сервіси безпеки міжмережевого екрану забезпечують виконання таких функцій захисту:

– надання достовірного каналу для введення атрибутів користувачів;

– ідентифікація та автентифікація користувачів на основі логіна та пароля;

– ведення журналів аудиту.

2.7.4.4 Сервіси безпеки ПЗ забезпечення цілісності) – це ПЗ програма, що дозволяє обчислювати значення хеш-сум (контрольних сум) файлів ПЗ міжмережевого екрану за алгоритмом MD5 та сигналізує у разі виявлення порушень. ПЗ забезпечення цілісності виконується на рівні ядра CentOS Linux v.7– RELEASE.

2.7.4.5 ПЗ антивірусного захисту забезпечує виконання таких функцій захисту:

– запобігання проникненню комп'ютерних вірусів;

– оперативне виявлення та знешкодження комп'ютерних вірусів у випадку їхнього проникнення;

– централізоване управління засобами антивірусного захисту з боку системного адміністратора;

– реєстрацію даних, що мають відношення до антивірусного захисту, аналіз звітів антивірусного ПЗ.

2.7.5 Апаратно-програмні засоби захисту

2.7.5.1 Використання апаратно-програмних засобів захисту інформації, Виробники якого мають сертифікати ISO 9001, забезпечує гарантії того, що вони:

– поставляються без несанкціонованих модифікацій;

– інсталюються і ініціюються Власником так, як це передбачається Виробником.

2.7.5.2 В документі [9] Додатку А визначено, що при побудові КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" для захисту інформації використовуються такі апаратно-програмні засоби захисту (далі – АПЗ):

– міжмережеве обладнання адміністративного сегменту;

– міжмережеве обладнання ЗВ ДМІ ТОВ "СІТЕЛ", яке розташоване на територіально розподілених майданчиках провайдера.

2.7.5.3 Міжмережеве обладнання адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ" - основний та резервний центральний комутатор Cisco Catalyst WS C3560G-24TS-S (далі комутатори Cisco Catalyst) забезпечує:

– ідентифікацію внутрішнього користувача ЗВ ДМІ ТОВ "СІТЕЛ" на основі політики авторизації (внутрішня IP-адреса);

– ідентифікацію процесів абонентів ЗВ ДМІ ТОВ "СІТЕЛ" на рівні IP-адреси, MAC-адреси відправника/одержувача;

– виконання перевірки стану обладнання та маршрутизації;

– реалізацію динамічного контролю ARP DAI (функція захисту від ARP spoofing атак. За допомогою ARP spoofing зловмисник посилає підроблене повідомлення на локальну мережу);

– контроль доступу до MAC-адреси.

2.7.5.4 До міжмережевого обладнання, яке безпосередньо розташоване на територіально розподілених майданчиках провайдера (вузлах) належить:

– комутаційне обладнання провайдера;

– маршрутизатори майданчика для підключення до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ".

2.7.5.5 Для забезпечення потреб окремих абонентів розгорнуті Підсистеми маршрутизації, до яких входять маршрутизатори ЗВ ДМІ ТОВ "СІТЕЛ". Підсистеми маршрутизації розміщуються в окремо відділених приміщеннях, що знаходяться під охороною.

2.7.5.6 Маршрутизатори забезпечують:

– ідентифікацію користувача на основі політики авторизації;

– самотестування при старті;

– реєстрацію подій;

– буферизацію з центральним вузлом системи, який з'єднує всі інші блоки один з одним;

– перевірку основних заголовків пакетів, що приходять на маршрутизатор (блок-пошук);

– налаштування пошуку маршруту.

2.7.5.7 "Перелік територіально розподілених майданчиків, включених до ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.ПІ.02" ([6] Додатку А), затверджено директором ТОВ "СІТЕЛ".

2.7.6 Засоби захисту, які мають експертні висновки за результатами державної експертизи у сфері ТЗІ

1) До засобів захисту, які мають Експертні висновки за результатами державної експертизи у сфері ТЗІ, належать:

– Експертний висновок № 723, дійсний з 15.05.2017 до 15.05.2020 на комплекс засобів захисту програмного забезпечення антивірусного захисту інформації ESET Gateway Security для Linux/BSD/Solaris версії 4. X, який реалізує такий функціональний профіль:

{КА-2, ЦА-1, ДР-1, ДС-1, ДЗ-1, НР-1, НИ-1,
НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1}

з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.

– Експертний висновок №771, дійсний з 20.10.2017 до 20.10.2020 на комутатори "Cisco Catalyst серій WS-C3560" під керуванням операційної системи IOS 15.x, який реалізує такий функціональний профіль:

{КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1,ДВ-1, НР-1,
НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1}

2) До засобів захисту, які потребують окремих експертних досліджень, належать засоби, які не мають Експертних висновків за результатами державної експертизи у сфері ТЗІ, а саме:

– сервіси безпеки ОС серверів;

– сервіси безпеки міжмережевого екрану;

– сервіси безпеки ПЗ забезпечення цілісності;

– сервіси безпеки ОС АПЗ:

- ОС Cisco Catalyst;
- ОС мережевого обладнання майданчиків провайдера.

2.7.7 Антивірусний захист інформації в ЗВ ДМІ ТОВ "СІТЕЛ"

ПЗ антивірусного захисту інформації реалізує такі функції захисту:

– організацію достовірного каналу для вводу початкових даних автентифікації адміністратора;

– автентифікацію адміністратора за паролем;

– централізоване управління засобами антивірусного захисту з боку системного адміністратора;

– реєстрацію даних, що мають відношення до антивірусного захисту, аналіз звітів антивірусного ПЗ;

– контроль власної цілісності і правильності функціонування.

Для антивірусного захисту використовується засоби, які мають позитивні Експертні висновки у сфері ТЗІ.

2.7.8 Функціональні специфікації комплексу засобів захисту інформації та рівень гарантій коректності реалізації функціональних послуг безпеки

Експертне оцінювання КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" здійснено відповідно до таких функціональних послуг безпеки, визначених у п. 5.4 ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ":

{КА-1, КА-2, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2}

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

Послуги безпеки, що реалізуються у КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", реалізовані з рівнем гарантій Г-2 згідно з НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

3 НОРМАТИВНІ ДОКУМЕНТИ, НА ВІДПОВІДНІСТЬ ВИМОГАМ ЯКИХ ЗДІЙСНЮЄТЬСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ

Експертиза КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" проведена з урахуванням вимог таких документів:

– Закон України "Про інформацію" від 2 жовтня 1992 року № 2657-XII (із змінами і доповненнями);

– Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року № 2594-IV;

– Указ Президента України №254/2017 від 30.08.2017р. "Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32.

– Указ Президента України №32/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації";

– 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 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі;

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

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

– ДСТУ 3396.0-96. Технічний захист інформації. Основні положення;

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

– Положення про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93. (у редакції наказу Адміністрації Держспецзв'язку України від 13.10.2017 № 565). Зареєстровано в Міністерстві юстиції України 16.07.2007 р. за № 820/14087.

4 МЕТОДИКА ПРОВЕДЕННЯ ЕКСПЕРТНИХ РОБІТ

Експертні роботи виконані згідно з документом "Державна експертиза комплексної системи захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Методика проведення експертизи. 33102567.62022.116.ПМ.01".

Методика проведення експертизи КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" погоджена встановленим порядком з Адміністрацією Держспецзв'язку.

5 ПЕРЕЛІК ДОКУМЕНТІВ, СКЛАД ПРОГРАМНИХ ТА ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТА ЕКСПЕРТИЗИ

5.1 Перелік документів на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", що наданий на експертизу, наведено у Додатку А.

5.2 В КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" використовуються такі сервіси безпеки ЗВ ДМІ ТОВ "СІТЕЛ" інформації:

– сервіси безпеки ОС серверів у складі:

- ОС серверу ME – CentOS Linux v.7– RELEASE;
- ОС серверу моніторингу – FreeBSD 9.2-STABLE;

– ПЗ антивірусного захисту – ESET Gateway Security для Linux/BSD/Solaris версії 4.5;

– сервіси безпеки міжмережевого екрану: набір попередньо сконфігурованих правил фільтрації трафіку абонентів, яке виконується на рівні ядра CentOS Linux v.7– RELEASE;

– сервіси безпеки ПЗ забезпечення цілісності - дозволяє обчислювати значення хеш-сум (контрольних сум) контролюючого файлу ПЗ міжмережевого екрану, що виконується а рівні ядра CentOS Linux v.7– RELEASE;

– сервіси безпеки ОС АПЗ у складі Cisco Catalyst – Cisco Catalyst WS C3560G-24TS-S.

6 РЕЗУЛЬТАТИ ЕКСПЕТНИХ РОБІТ

6.1 Результати аналізу документації, розробленої на етапі виконання перед проектних робіт

Документи, розроблені на етапі виконання перед проектних робіт наведені у п. А.1, Додатку А.

Склад, зміст та порядок затвердження документів, наданих Замовником, відповідає вимогам ДСТУ 3396.1-96, НД ТЗІ 1.4-001-2000 та включає:

– перелік інформації, що підлягає захисту під час її обробки в ЗВ ДМІ ТОВ "СІТЕЛ";

– політика безпеки;

– модель порушника;

– модель загроз інформації.

Перелік інформації, що підлягає захисту під час її обробки в ЗВ ДМІ ТОВ "СІТЕЛ" ([2] Додатку А) містить визначений перелік інформаційних ресурсів, що підлягають обробленню в ЗВ ДМІ ТОВ "СІТЕЛ", класифікований за семантичним вмістом, правовим режимом та режимом доступу, критичними властивостями інформації. Перелік оформлено у вигляді окремого документу та затверджено Директором ТОВ "СІТЕЛ".

Політика безпеки оформлена у вигляді розділу 3 документу Плану захисту інформації ([8] Додатку А) та містить відомості щодо:

– інформаційних ресурсів ЗВ ДМІ ТОВ "СІТЕЛ", які потребують захисту, основних загроз для інформації, компонентів обчислювальної системи, персоналу;

– захисту від загроз та політик забезпечення конфіденційності, цілісності, доступності оброблюваної інформації та спостережності ЗВ ДМІ ТОВ "СІТЕЛ";

– ПРД користувачів до інформаційних ресурсів ЗВ ДМІ ТОВ "СІТЕЛ", що потребують захисту, не суперечать результатам обстеження середовищ функціонування ЗВ ДМІ ТОВ "СІТЕЛ";

– правил, обмежень та рекомендацій, які регламентують порядок обробки інформації і спрямовані на захист інформації від визначених загроз з урахуванням наслідків їх реалізації.

Модель загроз інформації ([3] Додатку А), оформлена у вигляді окремого документу та містить перелік можливих типів загроз, класифікований за результатом впливу на інформацію, містить класифікований за визначеними ознаками перелік можливих способів реалізації загроз певного типу відносно різних інформаційних об'єктів ЗВ ДМІ ТОВ

"СІТЕЛ" у різному стані. Модель загроз інформації відповідає результатам обстеження середовищ функціонування ЗВ ДМІ ТОВ "СІТЕЛ" та прийнятій моделі потенційного порушника політики безпеки інформації в ЗВ ДМІ ТОВ "СІТЕЛ".

Модель порушника ([4] Додатку А), оформлена у вигляді окремого документа і містить неформалізований опис дій порушника, в якому визначено цілі порушника та їх градація за ступенями небезпечності для ЗВ ДМІ ТОВ "СІТЕЛ" та інформації, що потребує захисту, категорії персоналу, користувачів ЗВ ДМІ ТОВ "СІТЕЛ" та сторонніх осіб, із числа яких може бути порушник, класифікацію порушників за рівнем можливостей, які надаються їм засобами ЗВ ДМІ ТОВ "СІТЕЛ", визначення можливості або неможливості реалізації порушником певних загроз інформації з використанням уразливостей певних компонентів обчислювальної системи ЗВ ДМІ ТОВ "СІТЕЛ" або використовуваних програмних засобів. Модель порушника безпеки інформації в ЗВ ДМІ ТОВ "СІТЕЛ" відповідає результатам обстеження середовищ функціонування ЗВ ДМІ ТОВ "СІТЕЛ".

Склад, зміст та порядок затвердження представленої на експертизу документації ЗВ ДМІ ТОВ "СІТЕЛ", розробленої на етапі виконання перед проектних робіт, відповідає положенням чинної нормативно-правової бази в сфері ТЗІ, а також особливостям та умовам функціонування ЗВ ДМІ ТОВ "СІТЕЛ". Розроблені документи є взаємоузгодженими між собою.

6.2 Результати аналізу Технічного завдання на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"

Структура та зміст ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([5] Додатку А) відповідає вимогам НД ТЗІ 3.7-001-99.

При розробленні Технічного завдання враховані вимоги "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах", НД ТЗІ 1.1-002-99.

При розробленні Технічного завдання врахована структура ЗВ ДМІ ТОВ "СІТЕЛ", особливості її функціонування, а також завдання захисту, що мають вирішуватися створюваною КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", викладені у передпроектній документації.

ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" затверджене Директором ТОВ "СІТЕЛ" та погоджено Адміністрацією Держспецзв'язку від 04.11.2018р.

Розроблення та оформлення ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", його зміст, порядок погодження та затвердження відповідають положенням НД ТЗІ.

6.3 Результати оцінювання ФПБ, що реалізуються засобами захисту від НСД

Для кожної загрози із переліку, що визначений в Моделі загроз, забезпечується протидія однією або декількома функціями і послугами безпеки, що реалізуються, механізмами засобів захисту від НСД, які є сервісами безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", або організаційними та фізичними заходами захисту.

Елементи специфікації функцій кожної послуги безпеки (об'єкти захисту, процеси, користувачі, ролі, атрибути доступу, переліки подій та ресурсів тощо) є достатніми для реалізації вимог ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Вимоги до реалізації політики всіх ФПБ, наведені у п. 5.2 ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", а саме:

{КА-1, КА-2, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2}

Згідно з розглянутою проектною документацією КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" сукупність функціональних послуг безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" реалізується такими сервісами безпеки:

– сервіси безпеки ОС серверів у складі:

- ОС серверу МЕ – CentOS Linux v.7– RELEASE;
- ОС серверу моніторингу – FreeBSD 9.2-STABLE;

– сервіси безпеки міжмережевого екрану - набір попередньо сконфігурованих правил фільтрації трафіку абонентів, яке виконується на рівні ядра Linux (CentOS Linux v.7);

– сервіси безпеки ПЗ забезпечення цілісності - ПЗ md5sum яке дозволяє обчислювати значення хеш-сум (контрольних сум) контролюючого файлу (ПЗ міжмережевого екрану), що виконується на рівні ядра CentOS Linux v.7– RELEASE;

– сервіси безпеки ОС АПЗ ОС Cisco Catalyst- Cisco Catalyst WS C3560G-24TS-S;

– ПЗ антивірусного захисту - ESET Gateway Security для Linux/BSD/Solaris версії 4.5.

Перелік засобів захисту КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", які мають Експертні висновки за результатами державної експертизи у сфері ТЗІ, наведений у п.1 розділу.2.7.6.

Перелік сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", які не мають Експертних висновків за результатами державної експертизи у сфері ТЗІ, наведений у п.2 розділу.2.7.6 :

Для сервісів безпеки, які не мають Експертного висновку, шляхом вивчення технічної документації на ці компоненти ЗВ ДМІ ТОВ "СІТЕЛ" та проведення тестування, встановлено, що за своїм призначенням вони забезпечують захист інформації у КСЗІ ЗВ

ДМІ ТОВ "СІТЕЛ" у повному обсязі вимог ТЗ на створення ЗВ ДМІ ТОВ "СІТЕЛ", у частині, що стосується реалізації політик відповідних ФПБ (функцій захисту) визначених у функціональному профілі захищеності КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Коректну реалізацію зазначених нижче функціональних послуг безпеки забезпечує:

– наявність всіх сервісів безпеки, визначених у документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту.UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А);

– інсталяція, ініціалізація та експлуатація сервісів безпеки КСЗІ відповідно до вимог таких документів:

- Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Інструкція з адміністрування системи;
- Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Інструкція оператора мережевого обладнання.

6.3.1 НК-1. "Однонаправлений достовірний канал"

За результатами випробувань реалізації функціональної послуги безпеки "Достовірний канал" визнано її відповідність вимогам рівня *НК-1 - "Однонаправлений достовірний канал"* в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Реалізація політики послуги гарантує користувачу можливість безпосередньої взаємодії з такими КЗЗ та сервісами безпеки, визначеними у документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту" ([9] Додатку А):

– сервіси безпеки ОС серверів;

– ПЗ антивірусного захисту;

– сервіси безпеки міжмережевого екрану;

– сервіси безпеки ОС АПЗ.

6.4.1.1 Достовірний канал між користувачем та сервісів безпеки ОС серверів при першому вході ініціюється після монопольного відкриття пристроїв терміналу процесом, який виконує автентифікацію користувачів (login) до запуску будь-яких інших процесів, здатних взаємодіяти з користувачем, на екрані з'являється рядок Linux для введення логіну.

6.4.1.2 Достовірний канал між користувачем та ПЗ антивірусного захисту ініціюється шляхом запуску "системним адміністратором" ПЗ антивірусного захисту, після

чого з'являється вікно для вводу паролю доступу до облікового запису адміністратора, поза межами якого введення паролю неможливе.

6.4.1.3 Достовірний канал між користувачем та сервісами безпеки міжмережевого екрану ініціюється після монопольного відкриття пристроїв терміналу процесом, який виконує автентифікацію адміністраторів ЗВ ДМІ ТОВ "СІТЕЛ" (login) до запуску будь-яких інших процесів, здатних взаємодіяти з користувачем, з'являється вікно для введення пароля, поза межами якого введення паролю неможливе.

6.4.1.4 Достовірний канал між користувачем та сервісами безпеки ОС АПЗ шляхом введенням атрибутів доступу до сервісів безпеки ОС АПЗ ініціюється після монопольного відкриття пристроїв терміналу процесом, який виконує автентифікацію адміністраторів ЗВ ДМІ ТОВ "СІТЕЛ" (login) до запуску будь-яких інших процесів, здатних взаємодіяти з користувачем, з'являється вікно для введення логіну та пароля, поза межами якого введення логіну та паролю неможливе.

6.4.1.5 Введення атрибутів доступу для кожного апаратно–програмного засобу захисту КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується адміністратором при безпосередньому доступі до засобу захисту.

Достовірний канал ініціюється КЗЗ та сервісами безпеки тільки за запитом користувача.

6.3.2 НИ-2. "Одиночна ідентифікація і автентифікація"

За результатами випробувань реалізації функціональної послуги безпеки "Ідентифікація і автентифікація" визнано її відповідність вимогам рівня НИ-2 - *"Одиночна ідентифікація і автентифікація"* в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Реалізація політики послуги дозволяє визначити і перевірити особистість користувачів усіх категорій, що намагаються одержати доступ до ресурсів ЗВ ДМІ ТОВ "СІТЕЛ".

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту" ([9] Додатку А):

– визначені такі користувачі:

- користувачі – абоненти, яким надано право доступу тільки до загальнодоступної інформації WEB-ресурсів;
- користувачі, які забезпечують функціонування та адміністрування ЗВ ДМІ ТОВ "СІТЕЛ":
  - оператор мережного обладнання);

- системні адміністратори;
- адміністратори безпеки

– визначено, що політика послуги забезпечується такими КЗЗ та сервісами безпеки:

- сервіси безпеки ОС серверів;
- ПЗ антивірусного захисту;
- сервіси безпеки міжмережевого екрану;
- сервіси безпеки ОС АПЗ.

6.4.2.1 Сервіси безпеки ОС серверів однозначно автентифікує технічні засоби на підставі внутрішньої IP-адреси, а адміністраторів ЗВ ДМІ ТОВ "СІТЕЛ" на підставі паролю доступу.

6.4.2.2 ПЗ антивірусного захисту однозначно автентифікує користувача з роллю "системний адміністратор" за паролем доступу.

6.4.2.3 Сервіси безпеки міжмережевого екрану однозначно ідентифікують та автентифікують адміністраторів ЗВ ДМІ ТОВ "СІТЕЛ" на підставі логіну та паролю доступу.

6.4.2.4 Сервіси безпеки ОС АПЗ однозначно ідентифікують та автентифікують адміністраторів ЗВ ДМІ ТОВ "СІТЕЛ" на підставі внутрішньої IP-адреси, логіну та паролю.

6.4.2.5 КЗЗ та сервіси безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечують захист даних автентифікації від несанкціонованого ознайомлення, модифікації або руйнування.

6.3.3 НО-2. "Розподіл обов'язків"

За результатами випробувань реалізації функціональної послуги безпеки "Розподіл обов'язків" визнано її відповідність вимогам рівня НО-2 - "*Розподіл обов'язків адміністраторів*", в обсязі функцій, визначених ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги рівня НО-2 "Розподіл обов'язків" забезпечує керування можливостями користувачів і адміністраторів.

У документі "Пояснювальна записка до технічного проекту" ([9] Додатку А):

– визначені такі користувачі:

- користувачі – абоненти, яким надано право доступу тільки до загальнодоступної інформації WEB-ресурсів;
- користувачі, які забезпечують функціонування та адміністрування ЗВ ДМІ ТОВ "СІТЕЛ":
  - оператор мережного обладнання;
  - системні адміністратори;

- адміністратори безпеки;

– визначено, що політика послуги забезпечується такими КЗЗ та сервісами безпеки:

- сервіси безпеки ОС серверів;
- ПЗ антивірусного захисту;
- сервіси безпеки міжмережевого екрану;
- сервіси безпеки ОС АПЗ.

Функції користувачів наведені у п.2.2.2.1. Для кожної ролі Розробником визначені тільки ті функції, які необхідні для виконання даної ролі.

КЗЗ гарантують, що функції адміністраторів ніколи не можуть бути доступні користувачам.

Користувачеві надається можливість виступати в певній ролі адміністратора тільки після того, як він був автентифікований як користувач, якому надана певна роль адміністратора.

6.3.4 КА-1 "Мінімальна адміністративна конфіденційність"

За результатами випробувань реалізації функціональної послуги безпеки "Адміністративна конфіденційність" визнано її відповідність вимогам рівня КА-1 "Мінімальна адміністративна конфіденційність" в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги рівня КА-1 "Мінімальна адміністративна конфіденційність" надає спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів з метою захисту пасивних об'єктів захисту від несанкціонованого ознайомлення з їх вмістом (компрометації).

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А)::

– визначені такі об'єкти захисту:

- транзитна інформація мережного обладнання ЗВ ДМІ ТОВ "СІТЕЛ".

– визначено: Атрибутами доступу процесів до транзитної інформації абонентів ЗВ ДМІ ТОВ "СІТЕЛ" є:

- IP-адреса та MAC-адреса відправника/отримувача, вузла;
- таблиця маршрутизації пакетів.

– визначено: Атрибутами доступу процесів щодо фільтрації трафіку є:

- IP-адреси джерела і одержувача;

- тип транспортного протоколу;
- поля службових заголовків протоколів мережевого і транспортного рівнів;
- порт джерела і одержувачам;

– визначено, що політика послуги забезпечується такими сервісами безпеки:

- сервіси безпеки міжмережевого екрану;
- сервіси безпеки ОС АПЗ

6.4.4.1 Сервіси безпеки ОС АПЗ надають можливість операторам мережевого обладнання одержувати доступ до налаштувань щодо процесу передачі транзитної інформації абонентів ЗВ ДМІ ТОВ "СІТЕЛ".

6.4.4.2 Сервіси безпеки міжмережевого екрану дають можливість операторам мережевого обладнання одержувати доступ до налаштувань щодо процесу правил фільтрації трафіку ЗВ ДМІ ТОВ "СІТЕЛ".

Права доступу для кожного об'єкта захисту встановлюються в момент його створення.

6.3.5 КА-2. "Базова адміністративна конфіденційність"

За результатами випробувань реалізації функціональної послуги безпеки "Адміністративна конфіденційність" визнано її відповідність вимогам рівня КА-2 *"Базова адміністративна конфіденційність"* в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

6.3.5.1 Політика послуги рівня КА-2 "Базова адміністративна конфіденційність" дозволяє адміністраторам ЗВ ДМІ ТОВ "СІТЕЛ" керувати потоками інформації від захищених об'єктів до користувачів з метою захисту об'єктів захисту від несанкціонованого ознайомлення з їх вмістом.

6.3.5.2 У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А):

– визначені такі об'єкти захисту:

- технологічна інформація.

– визначені атрибути доступу:

- пароль до облікових записів сервісів безпеки ОС серверів;
- логін та пароль доступу до облікових записів сервісів безпеки міжмережевого екрану;
- пароль до облікових записів ПЗ антивірусного захисту;

- логін та пароль доступу до сервісів безпеки ОС АПЗ (ОС Cisco Catalyst, ОС мережевого обладнання майданчиків провайдера);
- внутрішня IP-адреса технічного засобу.

– визначені такі користувачі:

- оператор мережного обладнання;
- системні адміністратори;
- адміністратори безпеки;

– визначено, що політика послуги забезпечується такими КЗЗ та сервісами безпеки:

- сервіси безпеки ОС серверів;
- сервіси безпеки міжмережевого екрану;
- ПЗ антивірусного захисту;
- сервіси безпеки ОС АПЗ.

6.3.5.3 КЗЗ та сервіси безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" надають можливість адміністраторам:

– змінювати права доступу до об'єктів захисту;

– визначати користувачів або групи користувачів, які мають право читати об'єкти захисту;

– змінювати права доступу до програмних засобів КЗЗ та сервісів безпеки;

– визначати користувачів або групи користувачів, які мають право ініціювати процес.

Перевірка вважається успішною, якщо КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" обробляють запити на зміну прав доступу, що надходять від адміністраторів.

6.3.5.4 Сервіси безпеки ОС серверів здійснюють розмежування доступу до об'єктів захисту на підставі списків керування доступу, що встановлені користувачем з роллю "адміністратора безпеки" та внутрішньої IP-адреси.

6.3.5.5 Сервіси безпеки міжмережевого екрану здійснюють розмежування доступу на підставі ролей користувачів, внутрішньої IP-адреси та списків керування доступу, що встановлені користувачем з роллю "адміністратором безпеки".

6.3.5.6 ПЗ антивірусного захисту здійснює розмежування доступу до власних налаштувань на підставі належності користувача до ролі "системний адміністратор".

6.3.5.7 Сервіси безпеки ОС АПЗ здійснюють розмежування доступу до технологічної інформації та власних налаштувань на підставі належності користувача ролі "оператор мережевого обладнання", ролі "адміністратор безпеки" та внутрішньої IP-адреси.

Права доступу для кожного об'єкта захисту встановлюються в момент його створення.

6.3.6 ЦА-1. "Мінімальна адміністративна цілісність"

За результатами випробувань реалізації функціональної послуги безпеки "Адміністративна цілісність" визнано її відповідність вимогам рівня ЦА-1 - *"Мінімальна адміністративна цілісність"*, в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

6.3.6.1 Політика послуги рівня ЦА-1 "Мінімальна адміністративна цілісність" дозволяє адміністраторам ЗВ ДМІ ТОВ "СІТЕЛ" керувати потоками інформації від користувачів до захищених об'єктів з використанням засобів захисту з метою захисту пасивних об'єктів захисту від несанкціонованої модифікації.

6.3.6.2 У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А):

– визначені такі об'єкти захисту:
  - технологічна інформація.
– визначені атрибути доступу:
  - пароль до облікових записів сервісів безпеки ОС серверів;
  - логін та пароль доступу до облікових записів сервісів безпеки міжмережевого екрану;
  - пароль до облікових записів ПЗ антивірусного захисту;
  - логін та пароль доступу до сервісів безпеки ОС АПЗ (ОС Cisco Catalyst, ОС мережевого обладнання майданчиків провайдера);
  - внутрішня IP-адреса технічного засобу.
– визначені такі користувачі:
  - оператор мережного обладнання;
  - системні адміністратори;
  - адміністратори безпеки;
– визначено, що політика послуги забезпечується такими КЗЗ та сервісами безпеки:
  - сервіси безпеки ОС серверів;
  - сервіси безпеки міжмережевого екрану;
  - ПЗ антивірусного захисту;
  - сервіси безпеки ОС АПЗ.

6.3.6.3 КЗЗ та сервіси безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" надають можливість адміністраторам:

– змінювати права доступу до об'єктів захисту;

– визначати користувачів або групи користувачів, які мають право читати об'єкти захисту;

– змінювати права доступу до програмних засобів КЗЗ та сервісів безпеки;

– визначати користувачів або групи користувачів, які мають право ініціювати процес.

6.3.6.4 Сервіси безпеки ОС серверів здійснюють розмежування доступу до об'єктів захисту на підставі списків керування доступу, що встановлені користувачем з роллю "адміністратора безпеки" та внутрішньої IP-адреси.

6.3.6.5 Сервіси безпеки ОС серверів здійснюють розмежування доступу до сервісів безпеки міжмережевого екрану на підставі ролей користувачів, внутрішньої IP-адреси та списків керування доступу, що встановлені користувачем з роллю "адміністратором безпеки".

6.3.6.6 ПЗ антивірусного захисту здійснює розмежування доступу до власних налаштувань на підставі належності користувача до ролі "системний адміністратор".

6.3.6.7 Сервіси безпеки ОС АПЗ здійснюють розмежування доступу до технологічної інформації та власних налаштувань на підставі належності користувача ролі "оператор мережевого обладнання", ролі "адміністратор безпеки" та внутрішньої IP-адреси.

Права доступу для кожного об'єкта захисту встановлюються в момент його створення.

6.3.7 ЦА-2. "Базова адміністративна цілісність"

За результатами випробувань реалізації функціональної послуги безпеки "Адміністративна цілісність" визнано її відповідність вимогам рівня ЦА-2 - *"Базова адміністративна цілісність"*, в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

6.3.7.1 Політика послуги рівня ЦА-2 Базова адміністративна цілісність, що реалізується КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ", дозволяє адміністраторам керувати потоками інформації від пасивних об'єктів захисту до процесів з метою захисту пасивних об'єктів захисту від несанкціонованої модифікації.

6.3.7.2 У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А):

– визначені такі об'єкти захисту:

▪ транзитна інформація мережного обладнання ЗВ ДМІ ТОВ "СІТЕЛ".

– визначено: Атрибутами доступу процесів до транзитної інформації абонентів ЗВ ДМІ ТОВ "СІТЕЛ" є:

▪ IP-адреса та MAC-адреса відправника/отримувача, вузла;

▪ таблиця маршрутизації пакетів.

– визначено: Атрибутами доступу процесів щодо фільтрації трафіку є:

▪ IP-адреси джерела і одержувача;

▪ тип транспортного протоколу;

▪ поля службових заголовків протоколів мережевого і транспортного рівнів;

▪ порт джерела і одержувача;

– визначено, що політика послуги забезпечується такими сервісами безпеки:

▪ сервіси безпеки міжмережевого екрану;

▪ сервіси безпеки ОС АПЗ.

6.3.7.3 Сервіси безпеки ОС АПЗ надають можливість операторам мережевого обладнання одержувати доступ до налаштувань щодо процесу передачі транзитної інформації абонентів ЗВ ДМІ ТОВ "СІТЕЛ".

6.3.7.4 Сервіси безпеки міжмережевого екрану дають можливість операторам мережевого обладнання одержувати доступ до налаштувань щодо процесу правил фільтрації трафіку ЗВ ДМІ ТОВ "СІТЕЛ".

Права доступу для кожного об'єкта захисту встановлюються в момент його створення.

6.3.8 ЦО-1. "Обмежений відкат"

За результатами випробувань реалізації функціональної послуги безпеки "Відкат" визнано її відповідність вимогам рівня ЦО-1 – *"Обмежений відкат"*, в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

6.3.8.1 Політика послуги рівня ЦО-1 "Обмежений відкат", що реалізується КЗЗ та сервісами безпеки ЗВ ДМІ ТОВ "СІТЕЛ" забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.

6.3.8.2 У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А) визначено:

– об'єкти захисту, щодо яких забезпечується можливість відмінити операцію або послідовність операцій:

- технологічна інформація.

– політика послуги забезпечується такими сервісами безпеки та КЗЗ:

- сервіси безпеки ОС серверів;
- сервіси безпеки ОС АПЗ.

6.3.8.3 Сервіси безпеки ОС серверів мають засоби резервного копіювання, які дозволяють користувачеві з роллю "системний адміністратор" за відома користувача з роллю "адміністратор безпеки" відновити попередній стан об'єктів у файловій системі.

6.3.8.4 Сервіси безпеки ОС АПЗ мають засоби відновлення, які дозволяють користувачеві з роллю "адміністратор безпеки" відновити налаштувань КЗЗ (скидання до заводських налаштувань).

6.3.9 ДР–1. "Квоти"

За результатами випробувань реалізації функціональної послуги безпеки визнано її відповідність вимогам рівня ДР–1"Квоти", в обсязі фупкцій, визначених ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Реалізація політики послуги забезпечується такими сервісами безпеки: сервісами безпеки ОС сервера та сервісами безпеки міжмережевого екрану.

Політика послуги дозволяє забезпечити доступність послуг і ресурсів ЗВ ДМІ ТОВ "СІТЕЛ" шляхом керування обсягом ресурсів, що виділяються користувачам.

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД " ([9] Додатку А) визначено, що політика послуга відноситься до:

– перепускної здатності Серверів;

– процесорного часу;

Сервіси безпеки ОС сервера дозволяють накладати обмеження на кількість одночасних підключень з однієї IP-адреси до серверів та максимальний час виконання запитів, що надходять з віддаленого вузла.

Сервіси безпеки ОС сервера та сервіси безпеки міжмережевого екрану обробляють запити на зміну встановлених обмежень лише в тому випадку, якщо вони надходять від користувача з роллю "адміністратор безпеки".

На сервісах безпеки міжмережевого екрану налаштовано виявлення та відбиття атак типу "відмова у обслуговуванні", а також інших мережних атак

6.3.10 ДС-1. "Стійкість при обмежених відмовах"

За результатами випробувань реалізації функціональної послуги безпеки "Стійкість до відмов" визнано її відповідність вимогам рівня ДС-1 – "Стійкість при обмежених відмовах", в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги рівня ДС–1 "Стійкість при обмежених відмовах", що реалізується сервісами безпеки та КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", гарантує доступність ЗВ ДМІ ТОВ "СІТЕЛ" після відмови її компонента.

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А) визначені компоненти ЗВ ДМІ ТОВ "СІТЕЛ", відмови яких не призводять до недоступності ЗВ ДМІ ТОВ "СІТЕЛ".

Послуга застосовується до таких компонентів ЗВ ДМІ ТОВ "СІТЕЛ":

– АПЗ ЗВ ДМІ ТОВ "СІТЕЛ";

– система електроживлення адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ".

– сервіси безпеки ОС серверів;

– сервіси безпеки міжмережевого екрану;

– ПЗ антивірусного захисту

Відмова складових мережевого обладнання майданчика ЗВ ДМІ ТОВ "СІТЕЛ" не призводить до недоступності послуг ЗВ ДМІ ТОВ "СІТЕЛ".

Збої електричної мережі, у тому числі припинення енергопостачання адміністративного сегменту, не призводять до недоступності послуг ЗВ ДМІ ТОВ "СІТЕЛ". Резервне електроживлення забезпечується шляхом:

– включення резервного автоматичного джерела безперебійного живлення;

– підключення до дизельної генеруючої установки.

Сервіси безпеки та КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" повідомляють "адміністратора безпеки" про відмову будь-якого захищеного компонента.

6.3.11 ДЗ-1. "Модернізація"

За результатами випробувань реалізації функціональної послуги безпеки "Гаряча заміна" визнано її відповідність вимогам рівня ДЗ-1 – *"Модернізація"* в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги рівня ДЗ-1 "Модернізація" гарантує доступність ЗВ ДМІ ТОВ "СІТЕЛ" в процесі модернізації окремих компонентів.

У документі "Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Технологічна інструкція з модернізації. UA.31108855.КСЗІ.00001.И2.03" ([21] Додатку А): визначені політики проведення модернізації таких компонентів ЗВ ДМІ ТОВ "СІТЕЛ":

– програмні засоби:

- ОС серверів;
- сервіси безпеки міжмережевого екрану;
- ПЗ антивірусного захисту.

– комплекс технічних засобів:

- основний та резервний сервер міжмережевого екрану (далі - Сервер МЕ);
- сервер моніторингу;
- міжмережеве обладнання адміністративного сегменту;
- міжмережеве обладнання підсистеми маршрутизації;
- міжмережеве обладнання ЗВ ДМІ ТОВ "СІТЕЛ", яке розташоване на майданчиках провайдера.

Користувач з роллю "системний адміністратор" та "адміністратора безпеки" мають можливість провести модернізацію програмних та апаратних компонентів ЗВ ДМІ ТОВ "СІТЕЛ" без переривання виконання КЗЗ функцій захисту.

Модернізація, виконана у відповідності до порядку модернізації, не призводить до необхідності повторної інсталяції або переривання виконання КЗЗ функцій захисту.

Модернізація, виконана у відповідності до документу "Технологічна інструкція з модернізації", не призводить до переривання виконання КЗЗ функцій захисту.

6.3.12 ДВ-1. "Ручне відновлення"

За результатами випробувань реалізації функціональної послуги безпеки "Відновлення після збоїв" визнано її відповідність вимогам рівня ДВ-1 – "Ручне відновлення", в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги забезпечує повернення ЗВ ДМІ ТОВ "СІТЕЛ" у визначений у технічний документації стан після відмови або переривання обслуговування.

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проєкту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А) визначені:

– об'єкти, до яких відноситься послуга:

▪ відмова програмних та технічних (АПЗ) складових ЗВ ДМІ ТОВ "СІТЕЛ" внаслідок порушення цілісності або видалення їх складових (файлів, що виконуються, програмних бібліотек тощо);

– політика послуги забезпечується такими сервісами безпеки та КЗЗ:

▪ АПЗ ЗВ ДМІ ТОВ "СІТЕЛ";

▪ система електроживлення адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ".

▪ сервіси безпеки ОС серверів;

▪ сервіси безпеки міжмережевого екрану;

▪ ПЗ антивірусного захисту

Ручне відновлення компонент ЗВ ДМІ ТОВ "СІТЕЛ" виконується користувачами з ролями "адміністратор безпеки" та "системний адміністратор".

У режимі відновлення ЗВ ДМІ ТОВ "СІТЕЛ" користувач з роллю "адміністратор безпеки" здійснює супровід КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", які забезпечують:

– переведення системи у режими роботи (стани) системи, за яких можливе відновлення визначених об'єктів;

– повернення ЗВ ДМІ ТОВ "СІТЕЛ" у відомий захищений стан після завершення процедури відновлення.

Відмови, що стосуються даних абонентів ЗВ ДМІ ТОВ "СІТЕЛ", даних щодо трафіку абонента, усуваються користувачем з роллю "адміністратор безпеки" за допомогою ручних процедур із використанням резервних копій.

Відмови, що стосуються програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ", усуваються користувачем з роллю "системний адміністратор" під контролем адміністратора безпеки за допомогою ручних процедур із використанням резервних копій.

КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечують переведення у стан, з якого повернути його до нормального функціонування може користувач з роллю "адміністратор безпеки" та користувач з роллю "системний адміністратор".

При виникненні фізичного або логічного ушкодження областей постійних носіїв даних, де зберігаються елементи ОС, баз даних, журналів, конфігураційних чи керівних

файлів, антивірусного програмного забезпечення або загальносистемного програмного забезпечення, відновлення даних можливе за рахунок резервних серверів або системи резервування і відновлення функціонування ЗВ ДМІ ТОВ "СІТЕЛ".

Як ручні процедури, що дозволяють безпечним чином поновити функціонування компонентів системи при фізичному або логічному ушкодженні областей пам'яті, в яких зберігаються елементи ОС серверів, активного мережевого обладнання, розглядається перезавантаження обладнання, а у випадках істотних порушень в роботі – переінсталяція програмного забезпечення.

6.3.13 НР-2. "Захищений журнал"

За результатами випробувань реалізації функціональної послуги безпеки "Реєстрація" визнано її відповідність вимогам рівня НР-2 – *"Захищений журнал"*, в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги рівня НР-2 "Захищений журнал" дозволяє контролювати події, що стосуються безпеки інформації в ЗВ ДМІ ТОВ "СІТЕЛ".

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А):, визначено:

– політика послуги забезпечується такими сервісами безпеки та КЗЗ:

– сервіси безпеки ОС серверів;

– сервіси безпеки міжмережевого екрану;

– сервіси безпеки ОС АПЗ;

– ПЗ антивірусного захисту.

1) Сервіси безпеки ОС серверів здійснює реєстрацію таких подій:

– вхід та вихід користувачів з системи;

– невдалі спроби автентифікації;

– запуск та зупинка служб;

– помилки на рівні ОС;

– порушення цілісності або відмова компонентів;

– зміна атрибутів доступу користувачів.

2) Сервіси безпеки міжмережевого екрану здійснюють реєстрацію таких подій:

– підключення/відключення адміністраторів до засобів мережевого захисту з метою адміністрування;

– невдалі спроби підключення до обладнання та перевищення граничної кількості спроб введення пароля;

– факти надходження і відкидання інформаційних об'єктів (IP-пакетів), які не задовольняють встановленим правилам фільтрації IP-пакетів (спискам контролю доступу)

– спроби несанкційованого доступу до ресурсів мережі на рівнях L3-L7 моделі OSI.

3) ПЗ антивірусного захисту здійснює реєстрацію таких подій:

– порушення власної цілісності;

– відмова власних компонентів;

– оновлення вірусних баз;

– виявлені віруси та виконані дії відносно них.

4) Сервіси безпеки ОС АПЗ здійснюють реєстрацію таких подій:

– результати автентифікації при встановленні з'єднання;

– відомості щодо інспекції трафіка:

- ідентифікатор сесії абонента;
- час та місце підключення абонента;

– зміна налаштувань АПЗ;

– порушення власної цілісності;

– відмова власних компонентів;

– налаштування внутрішньої IP-адреси.

5) Усі записи про події містять інформацію про дату, час і тип події, успішність/неуспішність).

6) Записи про події аудита дій користувачів містять інформацію про користувача, процес і об'єкт.

7) Забезпечується захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнуванням.

8) КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується захист даних реєстрації від несанкціонованого доступу, модифікації або руйнування.

6.3.14 НЦ-1. "КЗЗ з контролем цілісності"

За результатами випробувань реалізації функціональної послуги безпеки "Цілісність комплексу засобів захисту" визнано її відповідність вимогам рівня НЦ-1 – *"КЗЗ з контролем цілісності"*, в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Політика послуги дозволяє визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

У документі "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД" ([9] Додатку А) визначено:

– склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.

– політика послуги забезпечується такими сервісами безпеки та КЗЗ:

- сервіси безпеки ОС серверів;
- сервіси безпеки ПЗ забезпечення цілісності;
- сервіси безпеки ОС АПЗ;
- ПЗ антивірусного захисту;

Сервіси безпеки ОС серверів забезпечують контроль цілісності файлів, що виконуються і файлів динамічних бібліотек (для яких була встановлена заборона на модифікацію).

ПЗ антивірусного захисту забезпечує виявлення та попередження спроб завершення власних процесів та модифікації власних файлів.

КЗЗ ОС АПЗ переводить апаратно-програмні компоненти ЗВ ДМІ ТОВ "СІТЕЛ" до стану, з якого повернути їх до нормального функціонування може тільки користувач з роллю "адміністратор безпеки".

Сервіси безпеки ПЗ забезпечення цілісності виконує набір тестів (з заданою періодичністю) з метою оцінки правильності хеш-сум (контрольних сум) файлів ПЗ міжмережевого екрану за алгоритмом MD5.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ" повідомляє адміністратора і (або) автоматично відновлює відповідність компонента еталону.

У разі неможливості відновлення своїх компонентів КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ" переводить ЗВ ДМІ ТОВ "СІТЕЛ" до стану, з якого повернути її до нормального функціонування можуть користувач з роллю "адміністратор безпеки" або користувач з роллю "системний адміністратор" під контролем адміністратора безпеки.

Послуги безпеки доступні тільки через інтерфейс КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ" і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

6.3.15 НТ-2. "Самотестування при старті"

За результатами випробувань реалізації функціональної послуги безпеки "Самотестування" визнано її відповідність вимогам рівня НТ-2 – "Самотестування при старті", в обсязі функцій, визначених у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та реалізованих у проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Реалізація політики послуги забезпечується такими компонентами сервісів безпеки та КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ":

– сервіси безпеки ОС серверів;

– сервіси безпеки ПЗ забезпечення цілісності;

– сервіси безпеки ОС АПЗ;

– ПЗ антивірусного захисту.

Політика послуги дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність множини функцій КЗЗ.

Тестування функцій сервісів безпеки ОС серверів з метою оцінки правильності власних конфігураційних файлів та цілісності власних компонентів забезпечується за запитом користувача з роллю "системний адміністратор" при ініціалізації КЗЗ.

ПЗ антивірусного захисту виконує набір тестів з метою оцінки правильності функціонування своїх критичних функцій за запитом користувача з роллю "системний адміністратор" та при ініціалізації КЗЗ та блокує виконання заражених файлів.

КЗЗ ОС АПЗ виконує набір тестів з метою оцінки правильності функціонування своїх критичних функцій та перевірки власних налаштувань в процесі функціонування при ініціалізації КЗЗ та за запитом користувача з роллю "адміністратор безпеки".

Сервіси безпеки ПЗ забезпечення цілісності виконує набір тестів (з заданою періодичністю) з метою оцінки правильності хеш-сум (контрольних сум) файлів ПЗ міжмережевого екрану за алгоритмом MD5. Сервіси безпеки ПЗ забезпечення цілісності виконує набір тестів при ініціалізації КЗЗ та за запитом користувача з роллю "адміністратор безпеки".

6.4 Результати оцінювання рівня гарантій Г2 коректності реалізації ФПБ КЗЗ КСЗІ

Рівень гарантій коректності реалізації ФПБ КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується діями Розробника на всіх стадіях життєвого циклу КСЗІ.

За результатами перевірки як розробленої документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", так і використаних Розробником КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" процедур і методик проектування та впровадження КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", які відповідають вимогам

стандартів серії ДСТУ ISO 9000 з використанням термінології з області керування якістю продукції (ДСТУ 3230-95), встановлено, що КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується рівень гарантій Г-2 реалізації послуг безпеки за рахунок дотримання вимог до:

– архітектури КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– середовища та послідовності розробки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– середовища функціонування та документування випробувань КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Вибрана архітектура КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідає структурі ЗВ ДМІ ТОВ "СІТЕЛ" і у змозі реалізувати політику безпеки, визначену у передпроектній документації на КСЗІ та у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ". Критичні для безпеки компоненти КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" захищені від не критичних для безпеки за рахунок використання механізмів захисту.

У процесі розробки визначені всі стадії життєвого циклу КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", які відповідають стадіям життєвого циклу ЗВ ДМІ ТОВ "СІТЕЛ", методика діяльності Розробника містить етапи робіт щодо створення складових КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та вимоги до них в частині захисту інформації, тобто процес розробки і супроводження КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" є повністю керованим з боку Розробника. Розробник розробив, запровадив і підтримує у робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки.

Підтверджується відповідність між проектом архітектури КЗЗ, визначеним у ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", та детальним проектом КЗЗ ЗВ ДМІ ТОВ "СІТЕЛ", а також забезпечуються гарантії того, що на кожній стадії розробки існує опис КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" і реалізація КСЗІ точно відповідає вихідним вимогам політики безпеки.

Забезпечуються гарантії того, що засоби КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" правильно реалізують політику безпеки і правильно функціонують, за рахунок наведення у експлуатаційній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" опису послуг безпеки, що реалізуються КЗЗ, переліку усіх можливих параметрів конфігурації засобів КЗЗ, які можуть використовуватися в процесі інсталяції, генерації і запуску.

КЗЗ оцінюваної КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" піддавався випробуванням. Розробник КЗЗ виконав тести з подолання механізмів захисту і довів, що КЗЗ відносно або абсолютно стійкий до різного роду атак. Доказом повноти випробувань є оформлені Протокол випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", який містить результати перевірки усіх КЗЗ, що реалізують послуги безпеки.

6.5 Результати аналізу проектної документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та матеріалів, які містять результати державної експертизи КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"

Проектна документація на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" наведена у розділах А2 та А.3 Додатку А..

Склад та зміст проектної документації відповідає вимогам вимогами ТЗ на ЗВ ДМІ ТОВ "СІТЕЛ", НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-2005 та відповідає умовам та особливостям функціонування ЗВ ДМІ ТОВ "СІТЕЛ", а також завданням захисту, що мають вирішуватися створюваною КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

У Пояснювальній записці до технічного проекту ([9] Додатку А): наведено відомості щодо:

– мети створення та призначення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– опису структури та складу ЗВ ДМІ ТОВ "СІТЕЛ";

– основних проектних рішень щодо побудови КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– рішень стосовно архітектури та складу КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– опису КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– рішень щодо налаштувань КЗЗ, що забезпечують реалізацію політики безпеки та правил доступу до інформації для кожної з ролей, визначених в ЗВ ДМІ ТОВ "СІТЕЛ";

– ідентифікації і автентифікації користувачів/процесів;

– реєстрації подій;

– рішень щодо функцій персоналу ЗВ ДМІ ТОВ "СІТЕЛ", порядку їх взаємодії;

– технічних рішень щодо підготовки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" до введення в дію;

– складу документів з проектування та розробки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Визначені у проектній документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" засоби захисту інформації за своїм призначенням придатні для захисту від НСД інформації в ЗВ ДМІ ТОВ "СІТЕЛ" у повному обсязі згідно з вимогами ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" у частині, що стосується реалізації політик відповідних ФПБ, визначених у функціональному профілі захищеності КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Проектна документація затверджена Директором ТОВ "СІТЕЛ".

План захисту інформації ([8] Додатку А) містить класифікацію інформації, що обробляється в ЗВ ДМІ ТОВ "СІТЕЛ", опис технології оброблення інформації в ЗВ ДМІ ТОВ "СІТЕЛ", опис моделі загроз для інформації в ЗВ ДМІ ТОВ "СІТЕЛ", опис політики безпеки інформації в ЗВ ДМІ ТОВ "СІТЕЛ", визначення завдань захисту інформації в ЗВ

ДМІ ТОВ "СІТЕЛ", визначення переліку документів, згідно з якими має здійснюватися захист інформації в ЗВ ДМІ ТОВ "СІТЕЛ", перелік і строки виконання робіт ВЗІ в ЗВ ДМІ ТОВ "СІТЕЛ".

План захисту інформації оформлений у вигляді окремого документа та затверджений Директором ТОВ "СІТЕЛ".

Матеріали, що містять результати державної експертизи (сертифікації) компонентів КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", і які наведені у п. А3 Додатку А

6.6 Результати аналізу експлуатаційної документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"

Експлуатаційна документація КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" наведена у п. А.4 Додатку А.

Експлуатаційна документація компонентів КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідає вимогам ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та складу сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", визначеному у проектній документації на КСЗІ

Для сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" зміст наданих документів положенням і рекомендаціям положенням чинної нормативно – правової бази в сфері ТЗІ.

Експлуатаційна документація на засоби захисту від НСД містить відомості щодо порядку безпечного конфігурування та використання усіх компонентів КЗЗ та КЗІ при реалізації всіх ФПБ, визначених у ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", у проектній документації на КСЗІ та НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-2005 та НД ТЗІ 2.7-010-09.

Інструкції з розгортання та експлуатації сервісів безпеки та КЗІ щодо порядку генерації ключових даних та поводження з ключовими документами містять опис засобів інсталяції, генерації та запуску компонентів сервісів безпеки та КЗІ, опис можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску системи, опис властивостей ЗВ ДМІ ТОВ "СІТЕЛ", які можуть бути використані для періодичної оцінки правильності функціонування сервісів безпеки та КЗІ, а також порядок генерації ключових даних та поводження з ключовими документами.

Інструкції з експлуатації та забезпечення безпеки експлуатації містять опис порядку використання функцій адміністрування для підтримки політики безпеки та забезпечення безпеки експлуатації сервісів безпеки в процесі функціонування ЗВ ДМІ ТОВ "СІТЕЛ" та її складових.

6.7 Результати аналізу нормативно-розпорядчої документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"

Нормативно-розпорядча документація на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" наведена у п. А.5 Додатку А.

Склад нормативно–розпорядчої документації відповідає ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та визначеним у проектній документації організаційним заходам, спрямованих на вирішення задач захисту інформації шляхом регламентації діяльності персоналу КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

У нормативно-розпорядчій документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" належним чином враховано положення КМУ від 29.03.2006 р. № 373, НД ТЗІ 1.4-001-2000, НД ТЗІ 1.1-002-99, які стосуються забезпечення захисту від НСД інформації, що обробляється в ЗВ ДМІ ТОВ "СІТЕЛ", та реалізації організаційних та інших заходів захисту, наведених в проектній документації на КСЗІ.

Положення Відповідального за захист інформації ([18] Додатку А):визначає завдання, функції, повноваження та відповідальність, порядок організації її робіт та взаємодії з іншими підрозділами, а також порядок її фінансування з урахуванням вимог постанови КМУ від 29.03.2006 р. № 373, НД ТЗІ 1.4-001-2000, НД ТЗІ 1.1-002-99 відповідає відомостям щодо особливостей ЗВ ДМІ ТОВ "СІТЕЛ" та умов її функціонування.

В технологічних (операційних) інструкціях (настановах) наведено:

– загальні положення, в яких визначено завдання з адміністрування та обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією;

– категорії співробітників ЗВ ДМІ ТОВ "СІТЕЛ", на яких поширюються вимоги відповідних інструкцій та які є відповідальними за виконання відповідних завдань;

– опис послідовності, правил та порядку здійснення технологічних операцій в ході виконання відповідальними особами певних завдань з адміністрування та обслуговування КСЗІ;

– опис порядку реєстрації фактів та результатів виконання певних завдань у відповідних реєстраційних журналах; форми використовуваних реєстраційних журналів.

Положення Відповідального за захист інформації ([18] Додатку А) та Технологічні (операційні) інструкції ([19] - [24] Додатку А) оформлені у вигляді окремих документів та затверджені директором ТОВ "СІТЕЛ".

6.8 Результати аналізу документації щодо проведених випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"

Документація щодо проведених випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" наведена п. А.6, Додатку А.

Програма та методика попередніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([25] Додатку А) містить перелік перевірок та опис методів (методик) виконання окремих перевірок згідно з вимогами ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", затверджена Директором ТОВ "СІТЕЛ".

Протокол проведення попередніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([27] Додатку А) містить задокументовані результати випробувань, передбачених програмою та методикою попередніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", висновки щодо можливості прийняття КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" в дослідну експлуатацію, підписаний членами комісії з проведення випробувань та затверджений Директором ТОВ "СІТЕЛ".

6.9 Результати аналізу організаційно-розпорядчої документації щодо впровадження КСЗІ

Організаційно-розпорядча документація щодо впровадження КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" наведена у п. А.7 Додатку А.

До складу організаційно-розпорядчої документації щодо впровадження КСЗІ відповідно до НД ТЗІ 3.7-003-2005, входять:

– Наказ Директора ТОВ "СІТЕЛ" про призначення комісії для проведення дослідної експлуатації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– Акти приймання у дослідну експлуатацію КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– Акти завершення дослідної експлуатації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– Акти завершення робіт зі створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Акт приймання у дослідну експлуатацію КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([28] Додатку А) містить задокументовані в "Протоколі проведення попередніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", відомості щодо результатів випробувань та висновки щодо можливості прийняття КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" в дослідну експлуатацію.

Акт приймання у дослідну експлуатацію КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" підписано членами комісії з проведення попередніх випробувань та затверджено Директором ТОВ "СІТЕЛ".

У Акті завершення дослідної експлуатації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([30] Додатку А) відображені результати дослідної експлуатації, а також наведені висновки щодо можливості надання КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" на державну експертизу.

Акт завершення дослідної експлуатації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" підписано членами комісії з проведення дослідної експлуатації та затверджено Директором ТОВ "СІТЕЛ".

Акт завершення робіт зі створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" ([31] Додатку А) містить відомості щодо етапів створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", проведених випробувань та висновки щодо завершення робіт зі створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Акт завершення робіт зі створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" підписаний виконавцями робіт зі створення КСЗІ та затверджений Директором ТОВ "СІТЕЛ".

6.10 Результати перевірки фактичного використання введених до складу КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" засобів захисту інформації

Склад наданої супровідної документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", перелік якої наведений у розділі А.8 Додатку А, відповідає ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та положенням чинних НД ТЗІ.

В результаті співставлення компонентів КЗЗ, визначених у проектній документації та зазначених у Формулярі ([32] Додатку А), встановлено, що визначені в проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" компоненти сервісів безпеки фактично інстальовані та ініціалізовані відповідно до положень експлуатаційної та нормативно–розпорядчої документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", про що є відповідні записи.

Налаштовані фактичні параметри всіх наявних компонентів сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідно до визначеного в експлуатаційної та нормативно – розпорядчої документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" порядку застосування відповідних компонентів КЗЗ при реалізації всіх ФПБ, визначених у ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Усі компоненти сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" знаходяться у працездатному стані та функціонують належним чином. При проведенні перевірок вимог до умов використання введених до складу сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" засобів захисту інформації, що не мають Експертного висновку, за результатами тестування було встановлено, що ці засоби забезпечують виконання функцій захисту інформації ЗВ ДМІ ТОВ "СІТЕЛ".

6.11 Результати перевірки порядку використання введених до складу КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" засобів захисту інформації

Склад та порядок створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам та виконання інших завдань з адміністрування та обслуговування КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідають положенням експлуатаційної документації ([12] - [17] Додатку А) та нормативно–розпорядчої документації ([18] - [24] Додатку А) КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Значення фактично призначених атрибутів доступу користувачів, процесів та захищених інформаційних ресурсів, які містяться у відповідних сховищах компонентів сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідають наведеним у відповідних реєстраційних журналах відомостям.

Зміст записів відповідних журналів реєстрації системних подій і подій безпеки, підтверджує факти належного застосування визначеного положеннями нормативно – розпорядчої документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" порядку створення захищених інформаційних ресурсів, реєстрації користувачів, надання прав доступу до інформації користувачам та виконання інших завдань з адміністрування та обслуговування КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Фактичні атрибути доступу користувачів, процесів та захищених інформаційних ресурсів у базі даних захисту КЗЗ КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідають змісту записів реєстраційних журналів.

6.12 Результати перевірки впровадження реалізованих у складі КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" організаційних, фізичних та інших заходів захисту

У складі КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" впроваджено всі організаційні, фізичні та інші нетехнічні заходи захисту, визначені у проектній та нормативно–розпорядчій документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Зміст наданої супровідної документації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" підтверджує факти належного застосування всіх впроваджених організаційних, фізичних та інших нетехнічних заходів захисту.

6.13 Результати перевірки підготовленості ВЗІ, персоналу та користувачів ЗВ ДМІ ТОВ "СІТЕЛ"

Співробітники, персонал та користувачі ЗВ ДМІ ТОВ "СІТЕЛ" ознайомлені під розпис з наказами та інструкціями, призначеними для ролей, які ці співробітники займають.

Співробітники, персонал та Користувачі впровадженої КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ":

– ознайомлені з основними положеннями експлуатаційної та нормативно-розпорядчої документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– пройшли інструктаж щодо використання сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ";

– мають достатній для виконання своїх посадових та функціональних обов'язків рівень практичних навичок щодо використання сервісів безпеки КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

Співробітники, персонал та користувачі ЗВ ДМІ ТОВ "СІТЕЛ" мають достатній для виконання своїх посадових та функціональних обов'язків рівень знань положень експлуатаційної та нормативно-розпорядчої документації на КСЗІ

6.14 Результати перевірки порядку розгортання територіально розподілених майданчиків Провайдера

Документація щодо умов та порядку розгортання та підключення територіально розподілених майданчиків провайдера наведена у розділі А.9 Додатку А.

Документ "Методика розгортання територіально розподілених майданчиків провайдера" ([24] Додатку А) містить такі основні положення:

– загальний порядок робіт, який включає:

▪ призначення комісії та призначення персоналу для розгортання та підключення вузла ЗВ ДМІ ТОВ "СІТЕЛ" до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ";

▪ визначення обсягу матеріалів (документів) необхідних для роботи Комісії, а також порядок передачі цих матеріалів;

▪ визначення порядку обліку вузла ЗВ ДМІ ТОВ "СІТЕЛ" у складі адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ";

– етапи розгортання територіально розподілених майданчиків провайдера, які включають:

▪ підбір та призначення персоналу;

▪ підготовка приміщення;

▪ підбір, закупівля або отримання у розпорядження апаратного та програмного забезпечення;

▪ налаштування комплексу технічних засобів;

▪ налаштування програмних засобів;

▪ налаштування комплексу засобів захисту;

▪ тестування правильності підключення вузла ЗВ ДМІ ТОВ "СІТЕЛ" до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ";

▪ завершення робіт з підключення вузла ЗВ ДМІ ТОВ "СІТЕЛ" до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ";

– підготовку документів на етапі підключення вузла ЗВ ДМІ ТОВ "СІТЕЛ", (шаблони яких наведені в Додатками в документі [24] Додатку А), які включають:

▪ розпорядчий документ "Протокол відповідності вимогам приміщення вузла ЗВ ДМІ ТОВ "СІТЕЛ"";

▪ розпорядчий документ "Перелік комутаційного обладнання мережевого обладнання вузла ЗВ ДМІ ТОВ "СІТЕЛ"";

▪ розпорядчий документ "Протокол тестування правильності підключення вузла ЗВ ДМІ ТОВ "СІТЕЛ" до адміністративного сегменту ЗВ ДМІ ТОВ "СІТЕЛ"";

▪ розпорядчий документ "Акт завершення робіт з розгортання територіально розподіленого майданчика провайдер".

Визначені у документі "Методика розгортання територіально розподілених майданчиків провайдера" ([24] Додатку А) засоби та заходи щодо розгортання територіально розподілених майданчиків Провайдера відповідають політиці безпеки, визначеної для КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", вимогам ТЗ на створення КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", проектній, експлуатаційній та іншій документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

7 ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ ЕКСПЕРТИЗИ

7.1 ЗВ ДМІ ТОВ "СІТЕЛ" – це захищений вузол доступу до мережі Інтернет.

7.2 В ЗВ ДМІ ТОВ "СІТЕЛ" забезпечується надання послуги "Захищений доступ до мережі Інтернет" ТОВ "СІТЕЛ" в частині забезпечення передачі даних між ресурсами мережі Інтернет (загальнодоступна інформація WEB-сторінок, HTLM-документи тощо і користувачами (абонентами).

7.3 ЗВ ДМІ ТОВ "СІТЕЛ" надає абонентам послугу "Захищений доступ до мережі Інтернет" яка дозволяє забезпечити:

– розподіл прав адміністратора ЗВБДМІ на керування потоками інформації від ресурсів мережі Інтернет через ЗВБДМІ до його користувачів (у тому числі абонентів);

– блокування ресурсів Інтернет по IP адресі за зверненням від користувача (абонента);

– надавання користувачам переліку сеансів зв`язку за вказаний період;

– аналіз потоків інформації за допомогою сервісів безпеки міжмережевого екрану.

– в випадку DDoS атаки блокування скомпрометованих IP адрес користувача, та надавання IP адреси з іншої мережі ТОВ "СІТЕЛ".

7.4 Згідно з "Переліком інформації, що підлягає захисту під час її обробки в інформаційно-телекомунікаційній системі ЗВ ДМІ ТОВ "СІТЕЛ", який затверджений директором ТОВ СІТЕЛ", в ЗВ ДМІ ТОВ "СІТЕЛ" обробляється відкрита інформація.

7.5 КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" створена з метою забезпечення захисту транзитної інформації абонентів захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ", відповідно до вимог Указу Президента України №254/2017 від 30.08.2017р. "Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13 лютого 2017 року № 32".

7.6 КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" – це сукупність організаційних та технічних заходів, технічних, програмних та програмно-апаратних засобів, які забезпечують захист інформації у відповідності до вимог ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ", у якому у повному обсязі та коректно враховані вимоги НД ТЗІ 1.1-002-99, НД ТЗІ 3.7-003-05, НД ТЗІ 3.7-001-99; та умови функціонування ЗВ ДМІ ТОВ "СІТЕЛ".

7.7 Реалізація КЗЗ та сервісів безпеки ЗВ ДМІ ТОВ "СІТЕЛ" вимог Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-

телекомунікаційних системах та інших чинних НД ТЗІ забезпечується таким профілями захищеності інформації:

{КА-1, КА-2, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2}

7.8 Сукупність функцій, реалізованих КЗЗ та сервісів безпеки ЗВ ДМІ ТОВ "СІТЕЛ" забезпечує реалізацію функціонального профілю захищеності інформації з рівнем гарантій Г2 згідно з НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

7.9 КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" забезпечує захист транзитної інформації абонентів за умови дотримання вимог та положень розроблених для КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" експлуатаційних та нормативно-розпорядчих документів.

7.10 Налаштування КЗЗ та сервісів безпеки ЗВ ДМІ ТОВ "СІТЕЛ" забезпечує реалізацію завдань захисту, викладених в ТЗ на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" та проектній документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

7.11 Склад та зміст документації на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" відповідає положенням чинної нормативно-правової бази у сфері ТЗІ, які стосуються захисту інформації з обмеженим доступом. Склад та зміст проектної та експлуатаційної документації є достатніми для забезпечення функціонування КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

7.12 Внутрішні користувачі ЗВ ДМІ ТОВ "СІТЕЛ" ознайомлені із документацією, призначеною для виконання функцій захисту.

7.13 Під час функціонування КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" можуть:

– вноситися зміни до технічних засобів та програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ";

– оновлюватися версії програмних та апаратно-програмних засобів захисту інформації.

– підключати територіально розподілені майданчики Провайдера.

8 ВИМОГИ ДО УМОВ ВИКОРИСТАННЯ ОБ'ЄКТА ЕКСПЕРТИЗИ

8.1 Введена в дію комплексна система захисту інформації в інформаційно-телекомунікаційній системі ТОВ "СІТЕЛ" повинна функціонувати відповідно до умов експлуатації, визначених у експлуатаційних та нормативно-розпорядчих документах на КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ".

8.2 КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" використовується за умови призначення Відповідального за захист інформації у ЗВ ДМІ ТОВ "СІТЕЛ"

8.3 Склад технічних засобів та встановленого програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ" повинен відповідати даним, що зазначені у Формулярах.

8.4 Усі роботи, пов'язані з модернізацією технічних засобів та програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ", повинні проводитися з урахуванням вимог документу "Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Технологічна інструкція з модернізації. UA.31108855.КСЗІ.00001.И2.03", вимог нормативно-правових актів та нормативних документів системи технічного захисту інформації.

8.5 Усі зміни у складі технічних засобів та встановленого програмного забезпечення ЗВ ДМІ ТОВ "СІТЕЛ", які не впливають на політику безпеки і не потребують додаткової експертизи, повинні бути задокументовані у Формулярах.

8.6 Оновлення версій програмних та апаратно-програмних засобів захисту інформації, що мають Експертний висновок та не суперечать прийнятій в КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" політиці безпеки, потребують проведення внутрішніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" в обсягах, що визначені Програмою та методикою попередніх випробувань, та оформлення відповідного Акту.

8.7 Усі роботи, пов'язані з підключенням додаткових територіально розподілених майданчиків Провайдера, повинні проводитися з урахуванням вимог документу "Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Методика розгортання територіально розподілених майданчиків провайдера. UA.31108855.КСЗІ.00001.И6" ([24] Додатку А).

9 ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії Експертного висновку – п'ять років з дати реєстрації Експертного висновку.

10 ОСОБЛИВІ ДУМКИ ЕКСПЕРТІВ

Протоколи експертизи не містять особливих думок експертів.

ДОДАТОК А.
ПЕРЕЛІК ДОКУМЕНТІВ, НАДАНИХ НА ЕКСПЕРТИЗУ КСЗІ ІТС СІТЕЛ

А.1 Документація, розроблена на стані виконання передпроектних робіт

[1] Наказ Директора ТОВ "СІТЕЛ" "Про створення комплексної системи захисту інформації" за №03 від 02.01.2018р.

[2] Перелік інформації, що підлягає захисту під час її обробки в ЗВ ДМІ ТОВ "СІТЕЛ". UA. 31108855.КСЗІ.00001.ПІ, затверджений Директором ТОВ "СІТЕЛ" від 19.01.2018р.

[3] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Модель загроз. Шифр – КСЗІ- ЗВ ДМІ ТОВ "СІТЕЛ".МЗ, від 19.10.2018р.

[4] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Модель порушника. Шифр – КСЗІ- ЗВ ДМІ ТОВ "СІТЕЛ".МП, від 19.10.2018р.

[5] Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Технічне завдання. Шифр – КСЗІ- ЗВ ДМІ ТОВ "СІТЕЛ".ТЗ, Затверджене Директором ТОВ "СІТЕЛ" від 22.10.2018р., Погоджене Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, від 04.11.2018р.

[6] Перелік територіально розподілених майданчиків, включених до ЗВБДМІ ТОВ "СІТЕЛ" UA.31108855.КСЗІ.00001.ПІ.02, від 20.02.2019р.

[7] Наказ Директора ТОВ "СІТЕЛ" "Про призначення відповідального за захист інформації та системного адміністратора" №05 від 04.03.2019р.

[8] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". План захисту інформації. UA.31108855.КСЗІ.00001.ЗП, від 04.03.2019р.

А.2 Проектна документація

[9] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Пояснювальна записка до технічного проекту. UA.31108855.КСЗІ.00001.ПД, від 04.03.2019р.

А.3 Матеріали, що містять результати державної експертизи (сертифікації) окремих компонентів (складових частин) КЗЗ КСЗІ

[10] Експертний висновок про відповідність вимогам нормативних документів системи технічного захисту інформації в Україні № 723 дійсний з 15.05.2017 до 15.05.2020 на Програмний продукт антивірусного захисту інформації ESET Gateway Security для Linux/BSD/Solaris версії 4.X (EGS).

[11] Експертний висновок про відповідність вимогам нормативних документів системи технічного захисту інформації в Україні №771, дійсний з з 20.10.2017 до 20.10.2020 на Комутатори "Cisco Catalyst серій WS-C3560" під керуванням операційної системи IOS 15.x.

А.4 Експлуатаційна документація

[12] Комплексна система захисту інформації захищеного вузла доступу до мережі інтернет ТОВ "СІТЕЛ". Інструкція з адміністрування системи. UA.31108855.КСЗІ.00001.И3, від 04.03.2019р.

[13] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Інструкція оператора мережевого обладнання. UA.31108855.КСЗІ.00001.И3.02, від 04.03.2019р.

[14] ESET GATEWAY SECURITY Installation Manual and User Guide (intended for product version 4.5 and higher) Linux and FreeBSD.

[15] Cisco DevNet Sandbox: Collaboration Labs LiveLessons.

[16] Использование интерфейса командной строки Cisco IOS – https://www.cisco.com

[17] Security Advisories, Responses and Notices - https://www.cisco.com

А.5 Нормативно-розпорядча документація

[18] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Положення про відповідального за захист інформації. UA.31108855.КСЗІ.00001.ПЗ, від 04.03.2019р., затверджено Наказом Директора ТОВ "СІТЕЛ", №06 від 04.03.2019р.

[19] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Інструкція щодо забезпечення режиму доступу під час обробки інформації в ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.И5, від 04.03.2019р.

[20] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Технологічна інструкція про порядок введення в експлуатацію КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.И2.02, від 04.03.2019р.

[21] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Технологічна інструкція з модернізації. UA.31108855.КСЗІ.00001.И2.03, від 04.03.2019р.

[22] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Технологічна інструкція щодо забезпечення функціонування КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ". UA.31108855.КСЗІ.00001.И2.04, від 04.03.2019р.

[23] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Технологічна інструкція з резервування та відновлення інформації в ЗВ ДМІ ТОВ "СІТЕЛ" . UA.31108855.КСЗІ.00001.И5, від 04.03.2019р.

[24] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Методика розгортання територіально розподілених майданчиків провайдера. UA.31108855.КСЗІ.00001.И6, від 04.03.2019р.

А.6 Документація щодо проведених випробувань

[25] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Програма та методика попередніх випробувань. UA.31108855.КСЗІ.00001.ПМ, від 04.03.2019р

[26] Наказ Директора ТОВ "СІТЕЛ" "Про призначення комісії для проведення попередніх випробувань" №07 від 05.03.2019р.

[27] Захищений вузол безпечного доступу до мережі Інтернет. Комплексна система захисту інформації. Протокол попередніх випробувань КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ" від 07.03.2019р.

А.7 Організаційно-розпорядча документація

[28] Акт приймання комплексної системи захисту інформації захищеного вузла безпечного доступу до мережі Інтернет ТОВ "СІТЕЛ", у дослідну експлуатацію", від 07.03.2019р.

[29] Наказ Директора ТОВ "СІТЕЛ" "Про призначення комісії для проведення дослідної експлуатації КСЗІ ЗВ ДМІ ТОВ "СІТЕЛ"" №08 від 11.03.2019р.

[30] Акт завершення дослідної експлуатації комплексної системи захисту інформаційно-телекомунікаційної системи ТОВ "СІТЕЛ" від 15.03.2019р.

[31] Акт завершення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі ТОВ "СІТЕЛ", від 15.03.2019р.

А.8 Супровідна документація

[32] Комплексна система захисту інформації захищеного вузла доступу до мережі Інтернет ТОВ "СІТЕЛ". Формуляр. UA.31108855.КСЗІ.00001.ФО, від 04.03.2019р.

[33] Журнал обліку фактів обслуговування, встановлення, технічних, апаратного та програмних засобів, від 04.03.2019р.

[34] Журнал створення резервних копій в ЗВ ДМІ ТОВ "СІТЕЛ", від 04.03.2019р.