1.	Предмет закупівлі (із зазначення коду національного класифікатора України ДК 021:2015 “Єдиний закупівельний словник”)	Послуги доступу до мережі Інтернет «ДК 021:2015 72410000-7 – Послуги провайдерів» **(UA-2026-02-02-011571-a)**
2.	Обґрунтування закупівлі (мета проведення закупівлі; правове забезпечення; проблеми, які будуть розв’язані в результаті закупівлі товарів, робіт, послуг)	Для забезпечення митних постів інтернетом та зв’язком
3.	Очікувана вартість закупівлі	Загалом: 133 580 грн. Лот №1 Послуги доступу до мережі інтернет (с. Нижанковичі, Самбірського р-ну., Львівської митниці, МАПП "Нижанковичі-Мальховіце"; с. Терло, Самбірський р-н, Львівська обл., МП "Смільниця"; с. Шегині, Львівська область, Яворівський район, МП " Шегині"): 47 122 грн. Лот №2 Послуги доступу до мережі інтернет (м. Львів, вул. Костюшка, 1; м. Львів, вул. Городоцька, 369; с. Грушів, Львівська обл., Яворівського р-н, МАПП "Грушів - Будомєж"; с. Рата, вул.Гребінського, 28, Львівський р-н, Львівська обл., МАПП "Рава-Руська - Хребенне"; смт. Краковець, вул. Михайла Вербицького, 54, Львівська обл., МАПП " Краківець – Корчова"): 55 044 грн. Лот №3 Послуги доступу до мережі інтернет (м. Броди, Золочівський район, Львівська обл., МП "Броди"): 15 707 грн. Лот №4 Послуги доступу до мережі інтернет (м. Шептицький, Львівська обл., МП "Сокаль"): 15 707 грн.
4.	Обґрунтування очікуваної вартості закупівлі (відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 “Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі”) *	Очікувану вартості закупівлі розраховано методом розрахунку очікуваної вартості товарів/послуг на підставі закупівельних цін попередніх закупівель (відповідно до методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 “Про затвердження примірної методики визначення очікуваної

		вартості предмета закупівлі”
5.	Технічні вимоги, технічне завдання (із зазначенням інформації про необхідні технічні, якісні та інші характеристики предмета закупівлі, у тому числі технічну специфікацію, умови експлуатації, технічне обслуговування, кількість товарів або обсяг виконаних робіт чи надання послуг)**	
6.	Чи включено предмет закупівлі до переліку товарів та послуг для централізованого забезпечення територіальних органів на рівні апарату Держмитслужби, затвердженого наказом Державної митної служби України від 25.05.2021 № 360 “Про затвердження Порядку підготовки показників проекту зведеного кошторису для складання бюджетного запиту, паспорта бюджетної програми та звіту про його виконання Державною митною службою України”.	Не включено

* може надаватися окремим додатком та разом з обґрунтуванням очікуваної вартості закупівлі надається специфікація із зазначенням вартості за одиницю Товару/Послуги
** може надаватися окремим додатком

Обґрунтування вартості послуг за предметом:

Код ДК 021:2015 72410000-7– Послуги доступу до мережі Інтернет

Очікувану вартості закупівлі розраховано методом розрахунку очікуваної вартості товарів/послуг на підставі закупівельних цін попередніх закупівель, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 “Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі”

1) Лот №1 Послуги доступу до мережі інтернет (с. Нижанковичі, Самбірського р-ну., Львівської митниці, МАПП "Нижанковичі-Мальховіце"; с. Терло, Самбірський р-н, Львівська обл., МП "Смільниця"; с. Шегині, Львівська область, Яворівський район, МП " Шегині"):

Посилання на попередню закупівлю: https://prozorro.gov.ua/uk/contract/UA-2025-04-01-008554-a-c1
Закупівля містить аналогічні послуги.

Індекс споживчих цін на різні товари та послуги до квітня попереднього року отриманий з сайту Держстату – 111,4%.

Очікувана вартість планованої закупівлі (три аналогічні послуги (територіально близькі) до послуги взазначеній закупівлі):

- Місце надання послуг: 82011, с. Нижанковичі, Самбірського р-ну., Львівської митниці, МАПП "Нижанковичі-Мальховіце"
- Місце надання послуг: 82069, с. Терло ,Самбірський р-н, Львівська обл.,МП

"Смільниця"

– Місце надання послуг: 81321, с. Шегині, Львівська область, Яворівський район, МП " Шегині"

3*14100*111,4% = 47 122 грн..

Всього: 47 122 грн..

2) Лот №2 Послуги доступу до мережі інтернет (м. Львів, вул. Костюшка, 1; м. Львів, вул. Городоцька, 369; с. Грушів, Львівська обл., Яворівського р-н, МАПП "Грушів - Будомєж"; с. Рата, вул.Гребінського, 28, Львівський р-н, Львівська обл., МАПП "Рава-Руська - Хребенне"; смт. Краковець, вул. Михайла Вербицького, 54, Львівська обл., МАПП " Краківець – Корчова"):

Посилання на попередню закупівлю: https://prozorro.gov.ua/uk/contract/UA-2025-02-14-005473-a-a1

Закупівля містить аналогічні послуги.

Індекс споживчих цін на різні товари та послуги до березня попереднього року отриманий з сайту Держстату – 111,2%.

Місце надання послуг:

- 79000, м. Львів, вул. Костюшка, 1.,
- 79040, м. Львів вул. Городоцька, 369,
- с. Грушів, Львівська обл., Яворівського р-н,
- с. Рата, вул. Гребінська, 28, Львівський р-н, Львівська обл.,
- смт. Краковець, вул. Вербицького, 54, Львівська обл., Яворівського р-н:

Очікувана вартість планованої закупівлі 49500*111,2% = 55 044 грн.

Всього: 55 044 грн..

3) Лот №3 Послуги доступу до мережі інтернет (м. Броди, Золочівський район, Львівська обл., МП "Броди"):

Посилання на попередню закупівлю: https://prozorro.gov.ua/uk/contract/UA-2025-04-01-008554-a-c1

Закупівля містить аналогічні послуги.

Індекс споживчих цін на різні товари та послуги до квітня попереднього року отриманий з сайту Держстату – 111,4%.

Очікувана вартість планованої закупівлі:

– Місце надання послуг: 80600, м. Броди, Бродівський район, Львівська обл., МП "Броди"

1*14100*111,4% = 15 707 грн..

Всього: 15 707 грн..

4) Лот №4 Послуги доступу до мережі інтернет (м. Шептицький, Львівська обл., МП "Сокаль"):

Посилання на попередню закупівлю: https://prozorro.gov.ua/uk/contract/UA-2025-04-01-008554-a-c1

Закупівля містить аналогічні послуги.

Індекс споживчих цін на різні товари та послуги до квітня попереднього року отриманий з сайту Держстату – 111,4%.

Очікувана вартість планованої закупівлі:

– Місце надання послуг: 80100, м. Шептицький, Львівська обл., МП "Сокаль"

1*14100*111,4% = 15 707 грн..

Всього: 15 707 грн.

Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі та технічна специфікація до предмета закупівлі

Послуги провайдерів, за кодом ДК 021:2015–72410000-7
(Послуги доступу до мережі Інтернет)

I. Лот №1 Послуги доступу до мережі інтернет (с. Нижанковичі, Самбірського р-ну., Львівської митниці, МАПП "Нижанковичі-Мальховіце"; с. Терло, Самбірський р-н, Львівська обл., МП "Смільниця"; с. Шегині, Львівська область, Яворівський район, МП " Шегині"):

1. Місце надання послуг:

с. Нижанковичі, Самбірського р-ну., Львівської митниці, МАПП "Нижанковичі-Мальховіце" (за межами території України на території Республіка Польща) – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

с. Терло ,Самбірський р-н, Львівська обл. ,МП "Смільниця" (за межами території України на території Республіка Польща) наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

с. Шегині, Львівська область, Яворівський район, МП " Шегині" – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

2. **Тип послуг:** Послуги провайдерів, за кодом ДК 021:2015–72410000-7 (Послуги доступу до мережі Інтернет) мають надаватися через Захищений вузол Інтернет доступу Учасника за технологією TCP/IP на швидкості відповідно переліку нижче та без урахування обсягів прийнятої та переданої інформації з операторським та технічним супроводженням доступу до мережі Інтернет:

3. Загальні вимоги:

3.1. Послуги доступу до мережі Інтернет (далі – Послуги) повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:

– Закону України «Про електронні комунікації»;

– Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 № 891;

– Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

– Правил надання та отримання електронних комунікаційних послуг, затверджених постановою Кабінету Міністрів України від 25 червня 2025 р. № 761 та інших нормативно-правових актів України у сфері телекомунікацій.

3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Учасника, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього.

3.3. Учасник здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлах мережі Замовника, відповідно до паспортних

характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Учасника.

3.4. Зона відповідальності Учасника при наданні Послуг – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання вузлів мережі, надається, встановлюється та налагоджується Учасником в рамках надання Послуг, та не використовується для інших цілей.

3.5. Доступ до мережі Інтернет повинен здійснюватися виключно з використанням волоконно-оптичних технологій без проміжних каналів, що використовують радіосигнал.

3.6. Прокладання окремого каналу зв'язку (за відсутності), підключення, вартість додаткового обладнання та комунікацій, інші видатки, пов’язані з наданням послуги, входять в загальну вартість закупівлі;

3.7. Учасник повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналів передачі даних, та у разі необхідності надавати ці відомості Замовнику.

3.8. Учасник повинен забезпечити технічну підтримку каналів передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.

3.9. У разі виникнення необхідності у Замовника різкого збільшення трафіку, Учасник повинен мати можливість тимчасово підвищити пропускну здатність по каналу доступу до мереж та ресурсів поза точкою обміну українським трафіком до 1 Гбіт/с (симетричний канал) за адресою: с. Нижанковичі, МАПП "Нижанковичі-Мальховіце", с. Терло, МП "Смільниця", с. Шегині, МП " Шегині".

3.10. Інтерфейс для прийому послуг: Ethernet (1000BASE-T, 1000BASE-TX, 100BASE-TX, 100BASE-T4).

3.11. Послуги надаються в режимі 24/7/365.

3.12. Учасник повинен мати пряме підключення не менше ніж до двох українських точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.13. Учасник повинен мати пряме підключення не менше ніж до двох зарубіжних точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.14. Затримка до українських точок обміну трафіком - не більше 10 мсек.

3.15. Затримка до європейських точок обміну трафіком (DE-CIX, PL-IX, AMS-IX) - не більше 45 мсек.

3.16. Втрата пакетів - не більше, ніж 0,1%.

3.17. Підключення до мережі Інтернет (включно з заведенням волоконно-оптичної лінії зв’язку в приміщення серверної кімнати замовника) у відповідності до всіх визначених технічних вимог має бути здійснено не пізніше 5календарних днів після укладення Договору.

4. Вимоги до Захищеного вузлу Інтернет доступу

Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Учасника із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.

Захищений вузол Інтернет доступу повинен являти собою сукупність програмно-технічних засобів та організаційних заходів для забезпечення доступу органів державної влади до мережі Інтернет із захистом інформаційних ресурсів відповідно до вимог законодавства України.

Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі ЗВІД повинен мати створену Комплексну систему захисту інформації з наступними функціями:

- застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;
- управління засобами захисту та функціями захисту активного мережевого обладнання, що входять до складу ЗВІД;

– безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;

– приймання повідомлень про інциденти щодо порушення безпеки від комплексу засобів захисту серверів ЗВІД;

– приймання повідомлень про інциденти щодо порушення безпеки від активних мережевих засобів захисту та обладнання;

– визначення правил проходження інформаційних потоків між активним мережевим обладнанням;

– захист програмно-апаратних засобів від несанкціонованого доступу;

– моніторинг та аналіз поточного стану безпеки ЗВІД;

– аналіз прийнятих повідомлень та сортування згідно з рангом загрози;

– контроль за входом користувачів в систему та доступом до ресурсів;

– реєстрація дій користувачів по відношенню до ресурсів системи;

– забезпечення цілісності інформаційних ресурсів центру (у тому числі антивірусний захист);

– перевірка цілісності та функціонування системи захисту;

– забезпечення необхідного рівня захисту технологічної інформації при її зберіганні, обробці, створенні та передачі за допомогою засобів системи, фізичний захист апаратно-програмних засобів ЗВІД від несанкціонованого доступу;

– контроль за цілісністю функціонального програмного забезпечення та даних;

– перевірка цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);

– забезпечення можливості повернення обчислювальної мережі ЗВІД у відомий захищений стан після відмов або переривання обслуговування;

– керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.

5. Вимоги до операторського та технічного супроводження.

5.1. Учасник повинен мати власний Центр технічної підтримки, що працює в режимі: 24x7x365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік) з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail);

5.2. Учасник має надати Замовнику контактні дані (службовий, мобільний телефон, електронна пошта, тощо) фахівців (не менше двох) відповідальних за надання послуг (у тому числі невідкладних).

5.3. Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Виконавця, та світових ресурсів.

5.4. Учасник повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.

5.5. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.

5.6. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо моніторингу протидії інцидентам з інформаційної безпеки на захищеному вузлі Учасник у реальному часі та за попередній період з моменту початку надання послуг.

5.7. Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 2 годин.

5.8. Учасник повинен мати можливість підтримки протоколу маршрутизації BGP.

5.9. Учасник повинен забезпечити усунення пошкоджень телекомунікаційної мережі та відновлення доступу до глобальної мережі у днів (далі - нормований час) відповідно до Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 28.12.2012 № 803 (зареєстрований в Міністерстві юстиції України 21.01.2013 за № 135/22667).

5.10. Учасник має бути включений до Реєстру операторів, провайдерів телекомунікацій.

6. Порядок та строки усунення інцидентів:

6.1. Відсутність надання послуг протягом 15 хвилин вважається інцидентом.

6.2. У випадку виникнення інцидентів Учасник негайно повідомляє про це представників технічної підтримки Замовника по телефону або за електронною поштою (e-mail).

6.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Учасника по телефону або через веб-сайт, або електронну пошту (e-mail).

6.4. Початком періоду інциденту вважається виявлена Учасником або Замовником відсутність надання послуг.

6.5. Строк усунення інцидентів, які виникли з вини Учасника, не повинен перевищувати 4 годин для м. Львів та 8 год для інших.

6.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.

6.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.

6.8. Про факт відновлення Послуг Учасник повідомляє Замовника по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Учасника Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.

6.9. Замовник зобов'язується надавати персоналу Учасника доступ до приміщень Замовника, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.

6.10. Для отримання необхідного доступу до приміщень Замовника, Учасник надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт.

6.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Учасника.

6.12. При надходженні заявки про інцидент (відсутність Послуги з вини Учасника), при перевищені строку відновлення надання Послуги понад нормований час, повинно бути припинене нарахування абонентської плати за період з моменту подачі заявки до відновлення надання Послуги у повному обсязі.

II. Лот №2 Послуги доступу до мережі інтернет (м. Львів, вул. Костюшка, 1; м. Львів, вул. Городоцька, 369; с. Грушів, Львівська обл., Яворівського р-н, МАПП "Грушів - Будомєж"; с. Рата, вул.Гребінського, 28, Львівський р-н, Львівська обл., МАПП "Рава-Руська - Хребенне"; смт. Краковець, вул. Михайла Вербицького, 54, Львівська обл., МАПП " Краківець – Корчова"):

1. **Місце надання послуг:**

м. Львів, вул. Костюшка, 1 – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 200 Мбіт/с, включення зі статичною IP – адресою);

м. Львів, вул. Городоцька, 369, наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

с. Грушів, Львівська обл., Яворівського р-н, МАПП "Грушів - Будомєж" (за межами території України на території Республіка Польща) – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

с. Рата, вул.Гребінського, 28, Львівський р-н, Львівська обл., МАПП "Рава-Руська - Хребенне" (на лінії держкордону) – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

смт. Краковець, вул. Михайла Вербицького, 54, Львівська обл., МАПП " Краківець – Корчова" (на лінії держкордону) – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

2. **Тип послуг:** Послуги провайдерів, за кодом ДК 021:2015–72410000-7 (Послуги доступу до мережі Інтернет) мають надаватися через Захищений вузол Інтернет доступу Учасника за технологією TCP/IP на швидкості відповідно переліку нижче та без урахування обсягів прийнятої та переданої інформації з операторським та технічним супроводженням доступу до мережі Інтернет:

3. **Загальні вимоги:**

3.1. Послуги доступу до мережі Інтернет (далі – Послуги) повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:

– Закону України «Про електронні комунікації»;

– Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 № 891;

– Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

– Правил надання та отримання електронних комунікаційних послуг, затверджених постановою Кабінету Міністрів України від 25 червня 2025 р. № 761 та інших нормативно-правових актів України у сфері телекомунікацій.

3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Учасника, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього.

3.3. Учасник здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлах мережі Замовника, відповідно до паспортних

характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Учасника.

3.4. Зона відповідальності Учасника при наданні Послуг – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання вузлів мережі, надається, встановлюється та налагоджується Учасником в рамках надання Послуг, та не використовується для інших цілей.

3.5. Доступ до мережі Інтернет повинен здійснюватися виключно з використанням волоконно-оптичних технологій без проміжних каналів, що використовують радіосигнал.

3.6. Прокладання окремого каналу зв'язку (за відсутності), підключення, вартість додаткового обладнання та комунікацій, інші видатки, пов’язані з наданням послуги, входять в загальну вартість закупівлі;

3.7. Учасник повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналів передачі даних, та у разі необхідності надавати ці відомості Замовнику.

3.8. Учасник повинен забезпечити технічну підтримку каналів передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.

3.9. У разі виникнення необхідності у Замовника різкого збільшення трафіку, Учасник повинен мати можливість тимчасово підвищити пропускну здатність по каналу доступу до мереж та ресурсів поза точкою обміну українським трафіком до 1 Гбіт/с (симетричний канал) за адресою: м. Львів, вул. Костюшка, 1.

3.10. Інтерфейс для прийому послуг: Ethernet (1000BASE-T, 1000BASE-TX, 100BASE-TX, 100BASE-T4).

3.11. Послуги надаються в режимі 24/7/365.

3.12. Учасник повинен мати пряме підключення не менше ніж до двох українських точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.13. Учасник повинен мати пряме підключення не менше ніж до двох зарубіжних точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.14. Затримка до українських точок обміну трафіком - не більше 10 мсек.

3.15. Затримка до європейських точок обміну трафіком (DE-CIX, PL-IX, AMS-IX) - не більше 45 мсек.

3.16. Втрата пакетів - не більше, ніж 0,1%.

3.17. Підключення до мережі Інтернет (включно з заведенням волоконно-оптичної лінії зв’язку в приміщення серверної кімнати замовника) у відповідності до всіх визначених технічних вимог має бути здійснено не пізніше 5календарних днів після укладення Договору.

4. Вимоги до Захищеного вузлу Інтернет доступу

Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Учасника із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.

Захищений вузол Інтернет доступу повинен являти собою сукупність програмно-технічних засобів та організаційних заходів для забезпечення доступу органів державної влади до мережі Інтернет із захистом інформаційних ресурсів відповідно до вимог законодавства України.

Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі ЗВІД повинен мати створену Комплексну систему захисту інформації з наступними функціями:

- застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;
- управління засобами захисту та функціями захисту активного мережевого обладнання, що входять до складу ЗВІД;

– безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;

– приймання повідомлень про інциденти щодо порушення безпеки від комплексу засобів захисту серверів ЗВІД;

– приймання повідомлень про інциденти щодо порушення безпеки від активних мережевих засобів захисту та обладнання;

– визначення правил проходження інформаційних потоків між активним мережевим обладнанням;

– захист програмно-апаратних засобів від несанкціонованого доступу;

– моніторинг та аналіз поточного стану безпеки ЗВІД;

– аналіз прийнятих повідомлень та сортування згідно з рангом загрози;

– контроль за входом користувачів в систему та доступом до ресурсів;

– реєстрація дій користувачів по відношенню до ресурсів системи;

– забезпечення цілісності інформаційних ресурсів центру (у тому числі антивірусний захист);

– перевірка цілісності та функціонування системи захисту;

– забезпечення необхідного рівня захисту технологічної інформації при її зберіганні, обробці, створенні та передачі за допомогою засобів системи, фізичний захист апаратно-програмних засобів ЗВІД від несанкціонованого доступу;

– контроль за цілісністю функціонального програмного забезпечення та даних;

– перевірка цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);

– забезпечення можливості повернення обчислювальної мережі ЗВІД у відомий захищений стан після відмов або переривання обслуговування;

– керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.

5. Вимоги до операторського та технічного супроводження.

5.1. Учасник повинен мати власний Центр технічної підтримки, що працює в режимі: 24x7x365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік) з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail);

5.2. Учасник має надати Замовнику контактні дані (службовий, мобільний телефон, електронна пошта, тощо) фахівців (не менше двох) відповідальних за надання послуг (у тому числі невідкладних).

5.3. Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Виконавця, та світових ресурсів.

5.4. Учасник повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.

5.5. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.

5.6. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо моніторингу протидії інцидентам з інформаційної безпеки на захищеному вузлі Учасник у реальному часі та за попередній період з моменту початку надання послуг.

5.7. Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 2 годин.

5.8. Учасник повинен мати можливість підтримки протоколу маршрутизації BGP.

5.9. Учасник повинен забезпечити усунення пошкоджень телекомунікаційної мережі та відновлення доступу до глобальної мережі у днів (далі - нормований час) відповідно до Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 28.12.2012 № 803 (зареєстрований в Міністерстві юстиції України 21.01.2013 за № 135/22667).

5.10. Учасник має бути включений до Реєстру операторів, провайдерів телекомунікацій.

6. Порядок та строки усунення інцидентів:

6.1. Відсутність надання послуг протягом 15 хвилин вважається інцидентом.

6.2. У випадку виникнення інцидентів Учасник негайно повідомляє про це представників технічної підтримки Замовника по телефону або за електронною поштою (e-mail).

6.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Учасника по телефону або через веб-сайт, або електронну пошту (e-mail).

6.4. Початком періоду інциденту вважається виявлена Учасником або Замовником відсутність надання послуг.

6.5. Строк усунення інцидентів, які виникли з вини Учасника, не повинен перевищувати 4 годин для м. Львів та 8 год для інших.

6.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.

6.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.

6.8. Про факт відновлення Послуг Учасник повідомляє Замовника по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Учасника Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.

6.9. Замовник зобов'язується надавати персоналу Учасника доступ до приміщень Замовника, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.

6.10. Для отримання необхідного доступу до приміщень Замовника, Учасник надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт.

6.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Учасника.

6.12. При надходженні заявки про інцидент (відсутність Послуги з вини Учасника), при перевищені строку відновлення надання Послуги понад нормований час, повинно бути припинене нарахування абонентської плати за період з моменту подачі заявки до відновлення надання Послуги у повному обсязі.

III. Лот №3 Послуги доступу до мережі інтернет (м. Броди, Золочівський район, Львівська обл., МП "Броди"):

1. Місце надання послуг:

м. Броди, Золочівський район, Львівська обл., МП "Броди"– наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

2. Тип послуг: Послуги провайдерів, за кодом ДК 021:2015–72410000-7 (Послуги доступу до мережі Інтернет) мають надаватися через Захищений вузол Інтернет доступу Учасника за технологією TCP/IP на швидкості відповідно переліку нижче та без урахування обсягів прийнятої та переданої інформації з операторським та технічним супроводженням доступу до мережі Інтернет:

3. Загальні вимоги:

3.1. Послуги доступу до мережі Інтернет (далі – Послуги) повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:

– Закону України «Про електронні комунікації»;

– Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 № 891;

– Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

– Правил надання та отримання електронних комунікаційних послуг, затверджених постановою Кабінету Міністрів України від 25 червня 2025 р. № 761 та інших нормативно-правових актів України у сфері телекомунікацій.

3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Учасника, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього.

3.3. Учасник здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлах мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Учасника.

3.4. Зона відповідальності Учасника при наданні Послуг – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання вузлів мережі, надається, встановлюється та налагоджується Учасником в рамках надання Послуг, та не використовується для інших цілей.

3.5. Доступ до мережі Інтернет повинен здійснюватися виключно з використанням волоконно-оптичних технологій без проміжних каналів, що використовують радіосигнал.

3.6. Прокладання окремого каналу зв'язку (за відсутності), підключення, вартість додаткового обладнання та комунікацій, інші видатки, пов’язані з наданням послуги, входять в загальну вартість закупівлі;

3.7. Учасник повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналів передачі даних, та у разі необхідності надавати ці відомості Замовнику.

3.8. Учасник повинен забезпечити технічну підтримку каналів передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.

3.9. У разі виникнення необхідності у Замовника різкого збільшення трафіку, Учасник повинен мати можливість тимчасово підвищити пропускну здатність по каналу доступу до мереж та ресурсів поза точкою обміну українським трафіком до 1 Гбіт/с (симетричний канал) за адресою: м. Броди, МП "Броди".

3.10. Інтерфейс для прийому послуг: Ethernet (1000BASE-T, 1000BASE-TX, 100BASE-TX, 100BASE-T4).

3.11. Послуги надаються в режимі 24/7/365.

3.12. Учасник повинен мати пряме підключення не менше ніж до двох українських точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.13. Учасник повинен мати пряме підключення не менше ніж до двох зарубіжних точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.14. Затримка до українських точок обміну трафіком - не більше 10 мсек.

3.15. Затримка до європейських точок обміну трафіком (DE-CIX, PL-IX, AMS-IX) - не більше 45 мсек.

3.16. Втрата пакетів - не більше, ніж 0,1%.

3.17. Підключення до мережі Інтернет (включно з заведенням волоконно-оптичної лінії зв’язку в приміщення серверної кімнати замовника) у відповідності до всіх визначених технічних вимог має бути здійснено не пізніше 5календарних днів після укладення Договору.

4. Вимоги до Захищеного вузлу Інтернет доступу

Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Учасника із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.

Захищений вузол Інтернет доступу повинен являти собою сукупність програмно-технічних засобів та організаційних заходів для забезпечення доступу органів державної влади до мережі Інтернет із захистом інформаційних ресурсів відповідно до вимог законодавства України.

Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі ЗВІД повинен мати створену Комплексну систему захисту інформації з наступними функціями:

- застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;
- управління засобами захисту та функціями захисту активного мережевого обладнання, що входять до складу ЗВІД;
- безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;
- приймання повідомлень про інциденти щодо порушення безпеки від комплексу засобів захисту серверів ЗВІД;
- приймання повідомлень про інциденти щодо порушення безпеки від активних мережевих засобів захисту та обладнання;
- визначення правил проходження інформаційних потоків між активним мережевим обладнанням;
- захист програмно-апаратних засобів від несанкціонованого доступу;
- моніторинг та аналіз поточного стану безпеки ЗВІД;
- аналіз прийнятих повідомлень та сортування згідно з рангом загрози;
- контроль за входом користувачів в систему та доступом до ресурсів;
- реєстрація дій користувачів по відношенню до ресурсів системи;
- забезпечення цілісності інформаційних ресурсів центру (у тому числі антивірусний захист);

– перевірка цілісності та функціонування системи захисту;

– забезпечення необхідного рівня захисту технологічної інформації при її зберіганні, обробці, створенні та передачі за допомогою засобів системи, фізичний захист апаратно-програмних засобів ЗВІД від несанкціонованого доступу;

– контроль за цілісністю функціонального програмного забезпечення та даних;

– перевірка цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);

– забезпечення можливості повернення обчислювальної мережі ЗВІД у відомий захищений стан після відмов або переривання обслуговування;

– керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.

5. Вимоги до операторського та технічного супроводження.

5.1. Учасник повинен мати власний Центр технічної підтримки, що працює в режимі: 24х7х365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік) з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail);

5.2. Учасник має надати Замовнику контактні дані (службовий, мобільний телефон, електронна пошта, тощо) фахівців (не менше двох) відповідальних за надання послуг (у тому числі невідкладних).

5.3. Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Виконавця, та світових ресурсів.

5.4. Учасник повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.

5.5. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.

5.6. Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо моніторингу протидії інцидентам з інформаційної безпеки на захищеному вузлі Учасник у реальному часі та за попередній період з моменту початку надання послуг.

5.7. Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 2 годин.

5.8. Учасник повинен мати можливість підтримки протоколу маршрутизації BGP.

5.9. Учасник повинен забезпечити усунення пошкоджень телекомунікаційної мережі та відновлення доступу до глобальної мережі у днів (далі - нормований час) відповідно до Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 28.12.2012 № 803 (зареєстрований в Міністерстві юстиції України 21.01.2013 за № 135/22667).

5.10. Учасник має бути включений до Реєстру операторів, провайдерів телекомунікацій.

6. Порядок та строки усунення інцидентів:

6.1. Відсутність надання послуг протягом 15 хвилин вважається інцидентом.

6.2. У випадку виникнення інцидентів Учасник негайно повідомляє про це представників технічної підтримки Замовника по телефону або за електронною поштою (e-mail).

6.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Учасника по телефону або через веб-сайт, або

електронну пошту (e-mail).

6.4. Початком періоду інциденту вважається виявлена Учасником або Замовником відсутність надання послуг.

6.5. Строк усунення інцидентів, які виникли з вини Учасника, не повинен перевищувати 4 годин для м. Львів та 8 год для інших.

6.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.

6.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.

6.8. Про факт відновлення Послуг Учасник повідомляє Замовника по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Учасника Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.

6.9. Замовник зобов'язується надавати персоналу Учасника доступ до приміщень Замовника, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.

6.10. Для отримання необхідного доступу до приміщень Замовника, Учасник надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт.

6.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Учасника.

6.12. При надходженні заявки про інцидент (відсутність Послуги з вини Учасника), при перевищені строку відновлення надання Послуги понад нормований час, повинно бути припинене нарахування абонентської плати за період з моменту подачі заявки до відновлення надання Послуги у повному обсязі.

IV. Лот №4 Послуги доступу до мережі інтернет (м. Шептицький, Львівська обл., МП "Сокаль"):

1. Місце надання послуг:

м. Шептицький, Львівська обл., МП "Сокаль" – наземний, симетричний (швидкість прийому та передачі інформації однакова - не менше 50 Мбіт/с);

2. Тип послуг: Послуги провайдерів, за кодом ДК 021:2015–72410000-7 (Послуги доступу до мережі Інтернет) мають надаватися через Захищений вузол Інтернет доступу Учасника за технологією TCP/IP на швидкості відповідно переліку нижче та без урахування обсягів прийнятої та переданої інформації з операторським та технічним супроводженням доступу до мережі Інтернет:

3. Загальні вимоги:

3.1 Послуги доступу до мережі Інтернет (далі – Послуги) повинні надаватися відповідно до чинних в Україні законодавчих та нормативних актів, зокрема:

– Закону України «Про електронні комунікації»;

– Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24.09.2001 № 891;

– Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;

– Правил надання та отримання електронних комунікаційних послуг, затверджених постановою Кабінету Міністрів України від 25 червня 2025 р. № 761 та інших нормативно-правових актів України у сфері телекомунікацій.

3.2 Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (далі – ЗВІД) Учасника, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього.

3.3 Учасник здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлах мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Учасника.

3.4 Зона відповідальності Учасника при наданні Послуг – до інтерфейсу локального мережевого обладнання вузла Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання вузлів мережі, надається, встановлюється та налагоджується Учасником в рамках надання Послуг, та не використовується для інших цілей.

3.5 Доступ до мережі Інтернет повинен здійснюватися виключно з використанням волоконно-оптичних технологій без проміжних каналів, що використовують радіосигнал.

3.6 Прокладання окремого каналу зв'язку (за відсутності), підключення, вартість додаткового обладнання та комунікацій, інші видатки, пов’язані з наданням послуги, входять в загальну вартість закупівлі;

3.7 Учасник повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик каналів передачі даних, та у разі необхідності надавати ці відомості Замовнику.

3.8 Учасник повинен забезпечити технічну підтримку каналів передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик.

3.9 У разі виникнення необхідності у Замовника різкого збільшення трафіку, Учасник повинен мати можливість тимчасово підвищити пропускну здатність по каналу доступу до мереж та ресурсів поза точкою обміну українським трафіком до 1 Гбіт/с (симетричний канал) за адресою: м. Шептицький, МП "Сокаль".

3.10 Інтерфейс для прийому послуг: Ethernet (1000BASE-T, 1000BASE-TX, 100BASE-TX, 100BASE-T4).

3.11 Послуги надаються в режимі 24/7/365.

3.12 Учасник повинен мати пряме підключення не менше ніж до двох українських точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.13 Учасник повинен мати пряме підключення не менше ніж до двох зарубіжних точок обміну трафіком зі швидкістю не менше 10 Гбіт/с.

3.14 Затримка до українських точок обміну трафіком - не більше 10 мсек.

3.15 Затримка до європейських точок обміну трафіком (DE-CIX, PL-IX, AMS-IX) - не більше 45 мсек.

3.16 Втрата пакетів - не більше, ніж 0,1%.

3.17 Підключення до мережі Інтернет (включно з заведенням волоконно-оптичної лінії зв'язку в приміщення серверної кімнати замовника) у відповідності до всіх визначених технічних вимог має бути здійснено не пізніше 5календарних днів після укладення Договору.

4. Вимоги до Захищеного вузлу Інтернет доступу

Доступ до глобальної мережі Інтернет повинен здійснюватися через власний Захищений вузол Інтернет-доступу (надалі – ЗВІД) Учасника із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки.

Захищений вузол Інтернет доступу повинен являти собою сукупність програмно-технічних засобів та організаційних заходів для забезпечення доступу органів державної влади до мережі Інтернет із захистом інформаційних ресурсів відповідно до вимог законодавства України.

Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі ЗВІД повинен мати створену Комплексну систему захисту інформації з наступними функціями:

- застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД;
- управління засобами захисту та функціями захисту активного мережевого обладнання, що входять до складу ЗВІД;
- безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту;
- приймання повідомлень про інциденти щодо порушення безпеки від комплексу засобів захисту серверів ЗВІД;
- приймання повідомлень про інциденти щодо порушення безпеки від активних мережевих засобів захисту та обладнання;
- визначення правил проходження інформаційних потоків між активним мережевим обладнанням;
- захист програмно-апаратних засобів від несанкціонованого доступу;
- моніторинг та аналіз поточного стану безпеки ЗВІД;
- аналіз прийнятих повідомлень та сортування згідно з рангом загрози;
- контроль за входом користувачів в систему та доступом до ресурсів;
- реєстрація дій користувачів по відношенню до ресурсів системи;
- забезпечення цілісності інформаційних ресурсів центру (у тому числі антивірусний захист);
- перевірка цілісності та функціонування системи захисту;

– забезпечення необхідного рівня захисту технологічної інформації при її зберіганні, обробці, створенні та передачі за допомогою засобів системи, фізичний захист апаратно-програмних засобів ЗВІД від несанкціонованого доступу;

– контроль за цілісністю функціонального програмного забезпечення та даних;

– перевірка цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);

– забезпечення можливості повернення обчислювальної мережі ЗВІД у відомий захищений стан після відмов або переривання обслуговування;

– керування мережевими засобами захисту та функціями захисту активного мережевого обладнання, що входить до складу ЗВІД.

5. Вимоги до операторського та технічного супроводження.

5.1 Учасник повинен мати власний Центр технічної підтримки, що працює в режимі: 24x7x365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік) з можливістю звернення по телефону або через веб-сайт, або електронну пошту (e-mail);

5.2 Учасник має надати Замовнику контактні дані (службовий, мобільний телефон, електронна пошта, тощо) фахівців (не менше двох) відповідальних за надання послуг (у тому числі невідкладних).

5.3 Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Виконавця, та світових ресурсів.

5.4 Учасник повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.

5.5 Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.

5.6 Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо моніторингу протидії інцидентам з інформаційної безпеки на захищеному вузлі Учасник у реальному часі та за попередній період з моменту початку надання послуг.

5.7 Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 2 годин.

5.8 Учасник повинен мати можливість підтримки протоколу маршрутизації BGP.

5.9 Учасник повинен забезпечити усунення пошкоджень телекомунікаційної мережі та відновлення доступу до глобальної мережі у днів (далі - нормований час) відповідно до Показників якості послуг із передачі даних, доступу до Інтернету та їх рівнів, затверджених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 28.12.2012 № 803 (зареєстрований в Міністерстві юстиції України 21.01.2013 за № 135/22667).

5.10 Учасник має бути включений до Реєстру операторів, провайдерів телекомунікацій.

6. Порядок та строки усунення інцидентів:

6.1 Відсутність надання послуг протягом 15 хвилин вважається інцидентом.

6.2 У випадку виникнення інцидентів Учасник негайно повідомляє про це представників технічної підтримки Замовника по телефону або за електронною поштою (e-mail).

6.3 У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Учасника по телефону або через веб-сайт, або електронну пошту (e-mail).

6.4 Початком періоду інциденту вважається виявлена Учасником або Замовником відсутність надання послуг.

6.5 Строк усунення інцидентів, які виникли з вини Учасника, не повинен перевищувати 4 годин для м. Львів та 8 год для інших.

6.6 Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку.

6.7 Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг.

6.8 Про факт відновлення Послуг Учасник повідомляє Замовника по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Учасника Замовник підтверджує чи не підтверджує факт відновлення надання Послуг.

6.9 Замовник зобов'язується надавати персоналу Учасника доступ до приміщень Замовника, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг.

6.10 Для отримання необхідного доступу до приміщень Замовника, Учасник надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт.

6.11 Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Учасника.

6.12 При надходженні заявки про інцидент (відсутність Послуги з вини Учасника), при перевищені строку відновлення надання Послуги понад нормований час, повинно бути припинене нарахування абонентської плати за період з моменту подачі заявки до відновлення надання Послуги у повному обсязі.