ПЕРЕЛІК ЗМІН

до тендерної документації щодо закупівлі послуг захищеного доступу до мережі Інтернет (основний канал) за ДК 021:2015 Єдиного закупівельного словника 72410000-7, Послуги провайдерів

1. Порівняльна таблиця

Стара редакція тендерної документації	Нова редакція тендерної документації
1. Загальні вимоги: 1.1. Послуги захищеного доступу до мережі Інтернет 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 вересня 2001 р. № 891/2001; - 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, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 7 липня 2008 р. за № 603/15294; - Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11 квітня 2012 р. № 295, та інших нормативно-правових актів України у сфері електронних комунікацій. 1.2. Відповідно до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» для забезпечення відмовостійкості об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинно здійснюватися (для об'єкта критичної інфраструктури, які надають свої послуги через Інтернет) зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами) (абзац сьомий пункту 38 Переліку базових вимог із забезпечення кіберзахисту об'єктів критичної	**1. Загальні вимоги:** 1.1. Послуги захищеного доступу до мережі Інтернет 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 вересня 2001 р. № 891/2001; - 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, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженого наказом Адміністрації Держспецзв'язку від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України 7 липня 2008 р. за № 603/15294; - Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11 квітня 2012 р. № 295, та інших нормативно-правових актів України у сфері електронних комунікацій. 1.2. Відповідно до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» для забезпечення відмовостійкості об'єкта критичної інформаційної інфраструктури об'єкт критичної інфраструктури повинно здійснюватися (для об'єкта критичної інфраструктури, які надають свої послуги через Інтернет) зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами) (абзац сьомий пункту 3 Переліку базових вимог із забезпечення кіберзахисту об'єктів критичної

інфраструктури додатку до Загальних вимог).	інфраструктури додатку до Загальних вимог).
2. Місце надання послуг: 54017, м. Миколаїв, вул. Маріупольська, 57-А.	**2. Місце надання послуг:** 54017, м. Миколаїв, вул. Маріупольська, 57-А.
3. Вимоги до послуг: 3.1. Тип послуг: послуги захищеного доступу до мережі Інтернет через Захищений вузол Інтернет доступу Виконавця за технологією TCP/IP по виділеній оптично-волоконній лінії зв'язку: за адресою м. Миколаїв, вул. Маріупольська, 57-А на швидкості 100 Мбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет: 3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (ЗВІД) Виконавця, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього. 3.3. Виконавець здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлі мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Виконавця. 3.4. Зона відповідальності Виконавця при наданні Послуг – до інтерфейсу локального мережевого обладнання Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання, надається, встановлюється та налагоджується Виконавцем в рамках надання Послуг, та не використовується для інших цілей. 3.5. Доступ до мережі Інтернет повинен здійснюватися за допомогою виділеного цифрового каналу передачі даних. Гарантована швидкість доступу до ресурсів мережі Інтернет за адресою м. Миколаїв, вул. Маріупольська, 57-А – для закордонних ресурсів 100 Мбіт/с на прийом та 100 Мбіт/с на передачу, без обмеження трафіку; – для українських ресурсів 100 Мбіт/с на прийом та 100 Мбіт/с на передачу, без обмеження трафіку;українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, бе 3.6. Виконавець повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних	**3. Вимоги до послуг:** 3.1. Тип послуг: послуги захищеного доступу до мережі Інтернет через Захищений вузол Інтернет доступу Виконавця за технологією TCP/IP по виділеній оптично-волоконній лінії зв'язку: за адресою м. Миколаїв, вул. Маріупольська, 57-А на швидкості 100 Мбіт/с без урахування обсягів прийнятої та переданої інформації, операторське та технічне супроводження доступу до мережі Інтернет; 3.2. Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через Захищений вузол Інтернет доступу (ЗВІД) Виконавця, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього. 3.3. Виконавець здійснює розміщення власного обладнання, необхідного для забезпечення надання Послуг на вузлі мережі Замовника, відповідно до паспортних характеристик обладнання, а Замовник забезпечує технічні умови для розміщення та експлуатації обладнання Виконавця. 3.4. Зона відповідальності Виконавця при наданні Послуг – до інтерфейсу локального мережевого обладнання Замовника. Відповідно все обладнання, включаючи кабелі до інтерфейсу локального мережевого обладнання, надається, встановлюється та налагоджується Виконавцем в рамках надання Послуг, та не використовується для інших цілей. 3.5. Доступ до мережі Інтернет повинен здійснюватися за допомогою виділеного цифрового каналу передачі даних. Гарантована швидкість доступу до ресурсів мережі Інтернет за адресою м. Миколаїв, вул. Маріупольська, 57-А – для закордонних ресурсів 100 Мбіт/с на прийом та 100 Мбіт/с на передачу, без обмеження трафіку; – для українських ресурсів 100 Мбіт/с на прийом та 100 Мбіт/с на передачу, без обмеження трафіку;українських ресурсів 200 Мбіт/с на прийом та 200 Мбіт/с на передачу, бе 3.6. Виконавець повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних

характеристик каналу передачі даних, та у разі необхідності надавати ці відомості Замовнику. 3.7. Виконавець повинен забезпечити технічну підтримку каналу передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик. 3.8. Інтерфейс для прийому послуг за адресою м. Миколаїв, вул. Маріупольська, 57-А: 100 Mbps Ethernet versions (100 BASE-T). 3.9. Послуги надаються в режимі 24/7/365. 3.10. Послуги повинні включати: – використання при наданні послуг механізму захисту від DDoS атак з застосуванням програмно-апаратного комплексу операторського рівня	характеристик каналу передачі даних, та у разі необхідності надавати ці відомості Замовнику. 3.7. Виконавець повинен забезпечити технічну підтримку каналу передачі даних, яка включає також постійний моніторинг каналу, діагностику причини відхилення від заданих технічних характеристик. 3.8. Інтерфейс для прийому послуг за адресою м. Миколаїв, вул. Маріупольська, 57-А: 100 Mbps Ethernet versions (100 BASE-T). 3.9. Послуги надаються в режимі 24/7/365. 3.10. **вилучений**
4.Вимоги до Захищеного вузлу Інтернет доступу. Захищений вузол Інтернет доступу (ЗВІД) – 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 (КСЗІ) з наступними функціями: – застосування політики безпеки на комплексі програмно-технічних засобів ЗВІД; – управління засобами захисту та функціями захисту активного мережевого обладнання що входить до складу ЗВІД; – безперервну експлуатацію та технічне обслуговування програмно-апаратних засобів захисту; – приймання повідомлень щодо інцидентів щодо порушення безпеки від Комплексу засобів захисту (КЗЗ) серверів ЗВІД; – приймання повідомлень щодо інцидентів з порушенням 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;	**вилучений**

– аналіз прийнятих повідомлень та сортування згідно рангу 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; – контроль за інсталяцією програмного забезпечення на серверах ЗВІД; – 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 (НСД); – контроль за цілісністю функціонального програмного забезпечення та даних; – контроль за запуском процесів та їх виконанням; – виявлення та реєстрацію спроб порушення прийнятих прав розмежування доступу; – виявлення та блокування розповсюдження шкідливих програм; – перевірки 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 програмно-апаратного комплексу захисту від DDoS атак. 5.1. Можливість відбиття атак рівня L3 (Volumetric), L4 (Infrastructure) і L7 (Application) мережевої моделі OSI. 5.2. Захист від Volumetric DDoS-атак на рівні пропускної спроможності аплінків та потужністю до 10 Гбіт/с для атак рівнів L4 та L7. 5.3. Активне придушення DDoS-атак в режимі реального часу. 5.4. Робота проти Volumetric і проти «Low and Slow» атак.	**вилучений**

5.5. Асиметричний режим роботи системи, тобто відсутність необхідності обробки вихідного трафіку для ефективного придушення DDoS атак. 5.6. Інтеграція з хмарним сервісом для отримання в реальному часі інформації про атаки, що відбуваються в світі, і засоби захисту від них. 5.7. Відсутність необхідності попереднього вивчення трафіку для створення профілю нормальної поведінки. 5.8. Розвинена система звітів і протоколювання всіх виконаних дій, що дозволяє відстежувати і коригувати можливі помилкові спрацьовування. 5.9. Автоматичне регулювання параметрів захисту з можливістю ручного регулювання параметрів системи в залежності від специфіки IT-системи Замовника. 5.10. On-line доступ Замовника до статистики та управління послугою. 5.11. Можливість виділення і збереження (на вимогу Замовника), зразків трафіку для подальшого їх аналізу Замовником.	
6. Вимоги до операторського та технічного супроводження. 6.1. Виконавець 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, через веб-сайт, електронну пошту (e-mail); 6.2. Виконавець повинен надати Замовнику перелік телефонів, веб-сайт та електронну пошту (e-mail) Центру технічної підтримки протягом 2-х календарних днів з моменту підписання Договору. 6.3. Звернення (повідомлення) Замовника повинно обов'язково включати: найменування Замовника; ім'я, прізвище, контактний телефон особи, що звертається; причину звернення. 6.4. На підставі звернення (повідомлення) Замовника Виконавець формує заявку, що включає всі відомості, повідомлені Замовником. 6.5. Виконавець повинен здійснювати постійний моніторинг каналу передачі даних, виявлення та усунення причин відхилення від заданих технічних характеристик. 6.6. У разі виявлення кіберінцинденту (кібератаки) на ресурси або трафік Замовника Виконавець повинен негайно повідомити про це представників технічної підтримки	**6. Вимоги до операторського та технічного супроводження.** 6.1. Виконавець 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, через веб-сайт, електронну пошту (e-mail); 6.2. Виконавець повинен надати Замовнику перелік телефонів, веб-сайт та електронну пошту (e-mail) Центру технічної підтримки протягом 2-х календарних днів з моменту підписання Договору. 6.3. Звернення (повідомлення) Замовника повинно обов'язково включати: найменування Замовника; ім'я, прізвище, контактний телефон особи, що звертається; причину звернення. 6.4. На підставі звернення (повідомлення) Замовника Виконавець формує заявку, що включає всі відомості, повідомлен Замовником. 6.5. Виконавець повинен здійснювати постійний моніторинг каналу передачі даних виявлення та усунення причин відхилення від заданих технічних характеристик. 6.6. У разі виявлення кіберінцинденту (кібератаки) на ресурси або трафік Замовника Виконавець повинен негайно повідомити про це представників технічної підтримки

Замовника по телефону та засобами електронної пошти (e-mail). 6.7. Виконавець повинен щомісячно надавати статистичну інформацію про послуги, що надаються. 6.8. Виконавець повинен забезпечити усунення пошкоджень каналу передачі даних та відновлення доступу до глобальної мережі у термін (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, зареєстрованого в Міністерстві юстиції України 21.01.2013 №135/22667.	Замовника по телефону та засобами електронної пошти (e-mail). 6.7. Виконавець повинен щомісячно надавати статистичну інформацію про послуги, що надаються. 6.8. Виконавець повинен забезпечити усунення пошкоджень каналу передачі даних та відновлення доступу до глобальної мережі у термін (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, зареєстрованого в Міністерстві юстиції України 21.01.2013 №135/22667.
7. Порядок та строки усунення інцидентів: 7.1. Відсутність надання послуг протягом 30 хвилин вважається інцидентом. 7.2. У випадку виникнення інцидентів Виконавець негайно повідомляє про це представників технічної підтримки Замовника по телефону та засобами електронної пошти (e-mail). 7.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Виконавця по телефону та засобами електронної пошти (e-mail). 7.4. Початком періоду інциденту вважається отримання Виконавцем від Замовника повідомлення про інцидент або повідомлення Виконавцем Замовника по телефону та засобами електронної пошти (e-mail). 7.5. Строк усунення інцидентів, які виникли з вини Виконавця не повинен перевищувати 2-х годин. 7.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку. 7.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг. 7.8. Про факт відновлення Послуг Виконавець повідомляє Замовника по телефону та дублює повідомлення на електронну пошту (e-mail). На повідомлення Виконавця Замовник підтверджує чи не підтверджує факт відновлення надання Послуг. 7.9. Замовник зобов'язується надавати персоналу Виконавця доступ до приміщень	**7. Порядок та строки усунення інцидентів:** 7.1. Відсутність надання послуг протягом 30 хвилин вважається інцидентом. 7.2. У випадку виникнення інцидентів Виконавець негайно повідомляє про це представників технічної підтримки Замовника по телефону та засобами електронної пошти (e-mail). 7.3. У випадку, якщо інцидент виявлено Замовником, останній негайно повідомляє про це представників технічної підтримки Виконавця по телефону та засобами електронної пошти (e-mail). 7.4. Початком періоду інциденту вважається отримання Виконавцем від Замовника повідомлення про інцидент або повідомлення Виконавцем Замовника по телефону та засобами електронної пошти (e-mail). 7.5. Строк усунення інцидентів, які виникли з вини Виконавця не повинен перевищувати 2-х годин. 7.6. Порядок та строки усунення інцидентів, що виникли з вини Замовника, погоджується Сторонами в кожному окремому випадку. 7.7. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг. 7.8. Про факт відновлення Послуг Виконавець повідомляє Замовника по телефону та дублює повідомлення на електронну пошту (e-mail). На повідомлення Виконавця Замовник підтверджує чи не підтверджує факт відновлення надання Послуг. 7.9. Замовник зобов'язується надавати персоналу Виконавця доступ до приміщень

Замовника, електронного комунікаційного обладнання, яке встановлено у Замовника відповідно п. 3.3, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг. 7.10. Для отримання необхідного доступу до приміщень Замовника, Виконавець надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт. 7.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Виконавця. 7.12. При надходженні заявки про інцидент (відсутність Послуги з вини Виконавця) 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.	Замовника, електронного комунікаційного обладнання, яке встановлено у Замовника відповідно п. 3.3, що забезпечує надання Послуг та розміщене в приміщеннях Замовника, для виконання робіт по відновленню Послуг. 7.10. Для отримання необхідного доступу до приміщень Замовника, Виконавець надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред'являє Замовнику службові посвідчення та направлення на виконання робіт. 7.11. Замовник має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Виконавця. 7.12. При надходженні заявки про інцидент (відсутність Послуги з вини Виконавця) 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.
8. **На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, Учасником у складі тендерної пропозиції надається:** 8.1. Довідка (форма довільна) щодо можливості надання послуг відповідно до вимог. 8.2. Довідку в довільній формі про організацію цілодобової технічної підтримки послуги (телефони «гарячої лінії», e-mail адреси, сайти технічної підтримки тощо). Інформація зазначена у довідці повинна бути підтверджена інформацією з офіційного сайту Учасника (за наявності). 8.3. Документ, який підтверджує внесення Учасника до реєстру операторів та/ або провайдерів телекомунікацій Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації. 8.4. На підтвердження відповідності системи захисту інформації Захищеного вузла Інтернет доступу (ЗВІД) встановленим вимогам у сфері захисту інформації учасник повинен надати копію дійсного Атестату відповідності виданого Державною службою спеціального зв'язку та захисту інформації України та	**8. На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, Учасником у складі тендерної пропозиції надається:** 8.1. Довідка (форма довільна) щодо можливості надання послуг відповідно до вимог. 8.2. Довідку в довільній формі про організацію цілодобової технічної підтримки послуги (телефони «гарячої лінії», e-mail адреси, сайти технічної підтримки тощо). Інформація зазначена у довідці повинна бути підтверджена інформацією з офіційного сайту Учасника (за наявності). 8.3. Документ, який підтверджує внесення Учасника до реєстру операторів та/ або провайдерів телекомунікацій Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації. 8.4. На підтвердження відповідності системи захисту інформації Захищеного вузла Інтернет доступу (ЗВІД) встановленим вимогам у сфері захисту інформації учасник повинен надати копію дійсного Атестату відповідності виданого Державною службою спеціального зв'язку та захисту інформації України та Експертного висновку до нього.

Експертного висновку до нього.	
8.5. Довідка (форма довільна), яка має містити інформацію про наявність програмно-апаратного комплексу захисту від DDoS атак, що відповідає вимогам указаним у пункті 5 Технічних вимог.	**8.5. Вилучений**
8.6. Документи, що підтверджують право власності або користування програмно-апаратним комплексом захисту від DDoS атак, або використання комплексу захисту від DDoS атак у вигляді «хмарного сервісу» від постачальника відповідних послуг.	**8.6. Вилучений**

2. До додатку 3 до Тендерної документації ПРОЕКТ ДОГОВОРУ внесено розділ щодо відповідальності сторін, а саме:

8. ВІДПОВІДАЛЬНІСТЬ СТОРІН

8.1. У випадку порушення своїх зобов'язань за цим Договором Сторони несуть відповідальність, визначену цим Договором та чинним законодавством України. Порушенням зобов'язання є його невиконання або неналежне виконання, тобто виконання з порушенням умов, визначених змістом зобов'язання.

8.2. Виконавець несе відповідальність:

8.2.1. за ненадання оплачених Послуг або надання їх в обсязі, меншому за оплачений - у розмірі оплаченої вартості ненаданих послуг та штрафу в розмірі 25 відсотків вартості послуг;

8.2.2. за безпідставне відключення кінцевого обладнання - у розмірі абонентної плати за весь період відключення

8.2.3. за безпідставні скорочення чи зміну переліку послуг - у розмірі абонентної плати за один місяць.

8.2.4. У разі не усунення протягом однієї доби із зафіксованого моменту подання Замовником заявки щодо пошкодження мережі, яке унеможливило доступ споживача до послуги або знизило до неприпустимих значень показники якості послуги, абонентна плата за весь період пошкодження не нараховується, а Виконавець у разі не усунення пошкодження протягом п'яти діб із зафіксованого моменту подання Замовником відповідної заявки сплачує Замовнику штраф у розмірі 25 відсотків добової абонентної плати за кожну добу перевищення цього терміну, але не більше ніж за три місяці.

8.3. Замовник несе відповідальність відповідно до статті 109 Закону України «Про електронні комунікації».

8.4. Сторони не несуть відповідальності за порушення своїх зобов'язань за цим Договором, якщо воно сталося не з їх вини. Сторона вважається невинуватою, якщо вона доведе, що вжила всіх залежних від неї заходів для належного виконання зобов'язання.

Старший державний інспектор підпис **Ірина КАБАЄВА**