***Додаток № 4***

***до тендерної документації***

**ПРОЄКТ ДОГОВОРУ № \_\_\_\_\_\_**про надання послуг

м. Київ «\_\_\_\_» \_\_\_\_\_\_\_\_ 20\_\_ року

**Бюджетна установа «Інформаційно-аналітичний центр дорожнього господарства** (далі – Абонент), в особі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(посада)\_\_(прізвище, ім’я, по батькові), який/яка діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(найменування документа, номер, дата та інші необхідні реквізити)\_\_\_\_\_\_\_\_\_\_ , з однієї сторони, та

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(найменування Оператора) (далі – Оператор), в особі ­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(посада)\_\_(прізвище, ім’я, по батькові), який/яка діє на підставі \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (найменування документа, номер, дата та інші необхідні реквізити)\_\_\_\_\_\_\_\_\_\_ з іншої сторони, що разом далі іменуються Сторони, а кожна окремо – Сторона, уклали цей договір (далі – Договір) про наступне:

1. Терміни, вживані в Договорі

**Послуги або Послуги Оператора** – послуги з надання некомутованого доступу до мережі Інтернет, що надаються Оператором в межах чинного Договору та додатків до нього, на підставі та відповідно до ліцензій, виданих Оператору Національною комісією, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку, або її правонаступниками (далі – НКЕК), та угодами з постачальниками послуг Оператору.

**Відключення** – набір технологічних операцій, що блокують Абоненту доступ до Послуг.

**Скасування** – набір операцій, що руйнує існуючий зв'язок. Для повторного ввімкнення необхідні процедури, аналогічні створенню нового Абонента.

**Розрахунковий період** – календарний місяць, у межах якого надавалися Послуги.

**Локальний Інтернет-реєстратор (LIR – Local Internet Registry)** – термін, який використовується для опису членів RIPE NCC. Їх називають локальними Інтернет-реєстраторами (LIR) тому що вони несуть відповідальність за розподіл адресного простору і реєстрацію адресного простору на локальному рівні. Локальні Інтернет-реєстратори також стверджують загальнообов'язкові політики і процедури на локальному рівні. Організації, які стають локальними Інтернет-реєстраторами – це в основному Інтернет-провайдери (ISP), які виділяють і призначають адресний простір своїм клієнтам, телекомунікаційні організації та комерційні підприємства поряд з академічними установами.

**Reseaux IP Europeens Network Coordination Centre (RIPE NCC)** є регіональною реєстратурою Інтернет для Європи, Близького Сходу і частини Центральної Азії який контролює розподіл і реєстрацію Інтернет-ресурсів в конкретному регіоні.

**Точка демаркації** – визначене фізичне місце/точка, де відповідальність за працездатність каналу переходить від однієї Сторони до іншої і в якій здійснюється фізичне і логічне з’єднання/підключення технічних засобів Провайдера транспортної послуги та відповідного обладнання зі сторони Абонента.

1. Предмет Договору
	1. В порядку та на умовах, визначених Договором, Оператор зобов’язується на

замовлення Абонента надавати послуги провайдеріввизначені за кодом **ДК 021:2015 – 72410000-7 Послуги провайдерів (****Послуги з надання доступу до захищеного вузла Інтернет-доступу (ЗВІД), підтримки блоку ір-адрес автономної системи (AS) та захист від DDoS-атак)** (далі – Послуги) відповідно до специфікації Додатку № 1 цього Договору, а Абонент зобов’язується прийняти та оплатити належним чином надані послуги.

* 1. Для забезпечення надання Послуг, за необхідності, Оператор може передати в

користування Абоненту комунікаційне обладнання (далі – Обладнання) на термін дії цього Договору. Передача Обладнання оформлюється Актом передачі-приймання обладнання. Після закінчення/припинення цього Договору Абонент повертає Обладнання Оператору, про що Сторони укладають відповідний акт.

* 1. Послуги надаються у відповідності до Закону України «Про електронні комунікації» (зі змінами), Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11.04.2012 № 295 (зі змінами) (далі – Правила) та інших нормативно-правових актів України та документів у сфері телекомунікацій.
	2. Оператор підтверджує, що його включено до реєстру операторів, провайдерів телекомунікацій (рішення про включення до реєстру від \_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_).
1. Ціна Договору
	1. Ціною даного Договору є загальна вартість Послуг наданих протягом терміну його дії, яка на момент його підписання становить \_\_\_\_\_ грн. 00 коп., в т.ч. ПДВ – \_\_\_\_ грн. 00 коп.

Вартість Послуги наданої протягом Розрахункового періоду становить \_\_\_\_\_\_\_\_ грн, у т.ч. ПДВ – \_\_\_\_\_\_\_\_ грн.

У разі, якщо Послуга надається не повний Розрахунковий період, її вартість розраховується шляхом ділення вартості Послуги за розрахунковий період на кількість всіх календарних днів Розрахункового періоду та множенням результату на кількість календарних днів Розрахункового періоду, протягом яких Послуга фактично надавалася.

Джерело фінансування: кошти Державного бюджету України.

* 1. Обсяги закупівлі Послуг можуть бути зменшені залежно від реального фінансування видатків.

У разі зменшення обсягів закупівлі ціна Договору може бути зменшена в залежності від потреб Абонента і в такому разі Сторони вносять відповідні зміни до Договору шляхом укладання додаткової угоди до цього Договору.

1. Права та обов’язки Сторін
	1. Оператор зобов'язується:
		1. Для забезпечення надання Послуг у встановлений термін провести підготовчі роботи з організації виділених цифрових каналів до майданчиків Абонента та підключити канали до своєї опорної цифрової мережі протягом 10 (десяти) робочих днів з дня укладення Договору.
		2. Надавати Абоненту Послуги відповідно до Технічних вимог, зазначених в Додатку № 2 та умовах цього Договору.
		3. Надавати Абоненту у визначені Договором строки інформацію щодо поточного стану взаєморозрахунків за цим Договором та змін вартості Послуг.
		4. Забезпечити усунення пошкоджень та відновлення працездатності Послуг по нормативах, встановлених діючими Правилами за рахунок Оператора.
		5. Застосовувати при наданні Послуг Абоненту обладнання і пристрої, що мають державні сертифікати.
		6. Не розголошувати відомості, одержані від Абонента в порядку виконання Договору, а також дані по переговорах Абонента, крім випадків, визначених чинним законодавством України.
		7. Приймати до розгляду скарги Абонента в порядку, встановленому діючими Правилами.
	2. Оператор має право:
		1. Своєчасно та в повному обсязі отримувати плату за надані Послуги відповідно до умов Договору.
		2. Один раз на 30 (тридцять) календарних днів проводити регламентні роботи на власній цифровій мережі не довше, ніж 2 (дві) години, протягом яких Абонент не буде мати можливості користуватися Послугою. При цьому Оператор не менш, ніж за 3 (три) доби попереджає Абонента про початок регламентних робіт в письмовій формі або електронною поштою, з метою узгодження зручного для Абонента часу проведення регламентних робіт.
		3. Відключити Абонента від мережі в разі порушення Абонентом законодавства України та норм міжнародного права, що стосуються інформації, її передачі та захисту, використання Послуги для розповсюдження забороненої інформації.
	3. Абонент зобов'язується:
		1. Своєчасно та в повному обсязі оплачувати належним чином надані Оператором Послуги відповідно до умов Договору.
		2. Виконувати рекомендації Оператора (фізичні інтерфейси, протоколи передачі даних і т.п.) по підключенню та використанню власного обладнання передачі даних, узгодивши попередньо його тип з Оператором.
		3. Припинити використання наданих Оператором IP-адрес з моменту припинення дії Договору.
		4. Повернути надані Оператором IP-адреси у випадку отримання статусу LIR (Local Internet Registry) протягом 14 (чотирнадцяти) календарних днів з моменту отримання такого статусу.
		5. У 20-денний строк повідомити Оператора про зміну юридичних або розрахункових реквізитів.
	4. Абонент має право:
		1. Достроково розірвати цей Договір, повідомивши про це Оператора не менше, ніж за 30 (тридцять) календарних днів до дня такого розірвання, за умови повного розрахунку з Оператором.
		2. Змінити місце надання Послуг в інші приміщення в межах зони дії мережі Оператора.
2. Відповідальність сторін
	1. Оператор несе відповідальність перед Абонентом в порядку і на умовах, визначених діючими законодавством України (Законом України «Про електронні комунікації», Правилами, іншими діючими нормативно-правовими актами, встановленими НКЕК та Кабінетом Міністрів України тощо).
	2. Оператор не несе відповідальності:
		1. За зміст інформації, що приймається, передається, обробляється та зберігається з використанням Послуги Оператора.
		2. За зміст інформації Абонента, що зберігається на сервері Оператора.
		3. За зниження якості Послуги з вини Абонента, перешкод в роботі, що виникають у прямий чи непрямий спосіб з причин, які знаходяться за межами контролю чи впливу Оператора.
		4. Перед третіми особами, якщо їм буде завдана шкода, пов'язана з використанням Послуг з вини Абонента.
		5. За якість функціонування окремих сегментів та вузлів глобальної мережі Інтернет, що знаходяться поза межами впливу Оператора.
		6. У випадку порушення Оператором терміну та/або порядку надання Послуг, визначених Договором, та/або в інших випадках, коли з будь-яких причин переривається термін надання Послуг, з Оператора стягується пеня в розмірі 0,1 % вартості Послуг за кожен день прострочення, а за прострочення понад 30 (тридцять) календарних днів додатково стягується штраф у розмірі 7 % вказаної вартості.
		7. За порушення Оператором умов щодо якості Послуг, Оператор сплачує Абоненту штраф у розмірі 20 % вартості неякісно наданих Послуг.
	3. Абонент несе відповідальність:
		1. За несвоєчасну оплату рахунків, що виставляються Оператором у вигляді пені у розмірі 0,1 % від несплаченої суми за кожен день прострочення. При цьому, при несплаті рахунку протягом наступних 10 (десяти) календарних днів, Оператор має право припинити надання Послуг.
		2. За достовірність відомостей, переданих Оператору в ході складання і виконання Договору.
		3. За використання пристроїв, які не мають сертифікатів та дозволу для використання на мережах зв’язку.
	4. Абонент звільняється від будь-якої відповідальності за порушення передбачених цим Договором термінів здійснення розрахунків, якщо такі порушення викликані відсутністю бюджетного фінансування (затримкою у бюджетному фінансуванні).
3. Порядок надання Послуг та проведення розрахунків
	1. Термін надання Послуг: цілодобово сім днів на тиждень з моменту підписання Договору до 31.12.2024 (включно).
	2. Місце надання Послуг визначені у Специфікації (Додаток 1 до цього Договору).
	3. Розрахунки за надані Послуги проводяться Абонентом щомісячно, шляхом оплати рахунку, що надається Оператором щомісячно разом з підписаним зі сторони Оператора Актом наданих Послуг (далі – Акт).
	4. Рахунки та Акти надаються Оператором не пізніше 5 (п’ятого) числа місяця, наступного за розрахунковим періодом.
	5. Абонент до 15 (п’ятнадцятого) числа місяця, наступного за розрахунковим періодом, повинен розглянути та, у випадку відсутності зауважень до наданих Оператором Послуг, підписати обидва примірники Акту і повернути один підписаний примірник зазначеного Акту Оператору.
	6. У разі незгоди Абонента підписати Акт (заперечення щодо правильності оформлення Акту, якості наданих Послуг чи з інших підстав), Абонент зобов’язаний в п’ятиденний строк офіційно направити Оператору відповідну мотивовану письмову відмову.
	7. Абонент сплачує за надані Послуги не пізніше 20 (двадцятого) числа місяця наступного після розрахункового періоду, за умови одержання рахунку та Акту від Оператора не пізніше 5 (п’ятого) числа місяця та відсутності зауважень згідно з п. 6.6. Договору.

У разі затримки/відсутності бюджетного фінансування, розрахунки здійснюються Абонентом у строк до 5 (п’яти) банківських днів з дати отримання відповідного фінансування.

* 1. При порушенні працездатності каналу зв’язку безперервно протягом 3 (трьох) годин з моменту звернення Абонента з цього приводу в сервісний центр Оператора, якщо таке порушення сталося з вини Оператора, вартість Послуг, що надаються на цьому напрямку за дану добу, виключається із щомісячної плати. Перерахунок здійснюється у наступному розрахунковому періоді.
1. Обставини непереборної сили
	1. Сторони погодились, що в разі виникнення дії обставин непереборної сили, яка не залежить від волі Сторін, а саме: війни, воєнного стану, антитерористичних операцій, блокади, ембарго, інших міжнародних санкцій, валютних обмежень, інших дій держав, які перешкоджають виконанню Сторонами своїх зобов'язань, пожеж, повеней, іншого стихійного лиха, Сторони звільнюються від виконання своїх зобов'язань на час дії зазначених обставин. У разі, коли дія зазначених обставин триває більш як 90 (дев’яносто) календарних днів, кожна із Сторін має право на розірвання Договору і не несе відповідальності за таке розірвання за умови, якщо вона повідомить про це іншу Сторону не пізніше як за 30 (тридцять) календарних днів до розірвання.
	2. Виникнення зазначених обставин не є підставою для Абонента для відмови оплатити Послуг, наданих до початку виникнення зазначених обставин. Якщо Сторони не виявили бажання розірвати Договір у зв`язку з виникненням зазначених обставин, після закінчення дії цих обставин відлік строків виконання зобов`язань за цим Договором продовжується.
	3. Належним доказом вищезазначених обставин та їх тривалості є документ Торгово-промислової палати України чи іншого компетентного органу.
2. **Антикорупційне застереження**
	1. Сторони погоджуються дотримуватися норм чинного законодавства України про запобігання корупції, про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, а також відповідних міжнародних актів та законодавства інших країн, дія якого розповсюджується на правовідносини Сторін за цим Договором.
	2. Сторони заявляють, що не здійснювали, не обіцяли, не уповноважували, не дозволяли, не пропонували (і зобов’язуються утримуватись від таких дій) у зв’язку з виконанням цього Договору, прямо чи опосередковано передачу або отримання будь-якого платежу, передачу будь-якої незаконної вигоди та/або здійснення незаконного впливу в інший спосіб щодо:
		1. будь-якої особи, на яку розповсюджується дія заборон/обмежень, передбачених законодавством України про запобігання корупції, про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення;
		2. будь-якої політичної партії, громадського об’єднання, засобу масової інформації;
		3. будь-якої особи, що є учасником, бенефіціаром (у тому числі, кінцевим), посадовою особою органів управління, працівником та/або уповноваженим представником іншої Сторони за цим Договором.
	3. Сторони зобов’язуються утримуватись від будь-яких дій, метою та/або результатом яких є порушення законодавства України про запобігання корупції, про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, вчинення злочинів у сфері господарської діяльності, а також докладати розумних зусиль для уникнення зазначених ризиків ділових відносин з відповідними контрагентами.
	4. Сторони підтверджують, що жодна з них, а також їх учасники, бенефіціари (у тому числі, кінцеві), посадові особи органів управління не були визнані винними у вчиненні і не вчиняли правопорушень, пов’язаних із корупцією, легалізацією (відмиванням) доходів, одержаних злочинним шляхом, фінансуванням тероризму та фінансуванням розповсюдження зброї масового знищення, злочинів у сфері господарської діяльності.
	5. Сторони підтверджують, що на них, а також на їх учасників, бенефіціарів (у тому числі, кінцевих), посадових осіб органів управління не поширюється дія національних санкцій України, санкцій Ради безпеки ООН, Європейського Союзу, Відділу з контролю за іноземними активами Державного казначейства США, Департаменту торгівлі Бюро промисловості та безпеки США, Державного департаменту США, Сполученого Королівства Великої Британії та Північної Ірландії або будь-якої іншої держави чи міжнародної організації, які можуть призвести до ризиків діяльності іншої Сторони (в тому числі реалізації правовідносин за цим Договором).
3. Додаткові умови і інші положення
	1. Умови чинного Договору можуть бути переглянуті за згодою Сторін з обов'язковим оформленням відповідної додаткової угоди до цього Договору.
	2. Істотні умови Договору не можуть змінюватися до виконання зобов’язань Сторонами в повному обсязі, за винятком умов, визначених пунктом 19 Особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 (девяносто) днів з дня його припинення або скасування, затверджених постановою Кабінету Міністрів України від 12.10.2022 № 1178.
	3. Договір залишається чинним при зміні реквізитів Сторін, їх реєстраційних документів, враховуючи зміну власника, організаційно-правової форми тощо, якщо ці зміни були виконані з дотриманням усіх вимог до умов передачі правонаступництва.
	4. Підписанням даного Договору, Абонент надає згоду на те, що інформація про нього буде внесена до бази даних Оператора. Абонент надає згоду Оператору на використання та обробку персональних даних, та погоджується з тим, що ця інформація буде використовуватись для обліку Абонентів, обліку наданих Послуг, а також для розрахунків та розсилання повідомлень і рахунків на сплату Послуг.
	5. Всі додаткові угоди та додатки складають невід'ємну частину Договору.
	6. Оператор забезпечує приймання, реєстрацію та оперативний розгляд претензій Абонента представниками власного сервісного центру за телефоном \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а також гарантує впровадження відповідних заходів щодо відновлення якості послуг у строки, відповідно з діючими нормативними документами, встановленими НКЕК та Кабінетом Міністрів України.
4. Порядок вирішення спорів
	1. У випадку виникнення спорів або розбіжностей Сторони зобов’язуються вирішувати їх шляхом взаємних переговорів та консультацій.
	2. У разі недосягнення Сторонами згоди, спори (розбіжності) вирішуються у судовому порядку відповідно до чинного законодавства України.
5. Термін дії Договору
	1. Цей Договір набирає чинності з дати його підписання обома Сторонами і діє до 31.12.2024, а в частині розрахунків – до повного їх виконання.
6. Додатки до договору
	1. Невід’ємною частиною цього Договору є:
		1. Додаток № 1 – Специфікація послуг.
		2. Додаток № 2 – Технічні вимоги.
		3. Додаток № 3 – Відповідальні представники сторін.
7. **Реквізити сторін**

|  |  |
| --- | --- |
| АБОНЕНТ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** | ОПЕРАТОР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** |
|  |  |

Додаток 1 до Договору
від \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

**СПЕЦИФІКАЦІЯ ПОСЛУГ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Найменування послуги | Параметри | Період | Ціна, грн без ПДВ/міс. | Сума, грн без ПДВ |
| 1. | Послуги захищеного доступу до мережі Інтернет без обмеження спожитого трафіку через Захищений вузол Інтернет доступум. Київ, вул. Антоновича, будинок 51 | 3 000/3 000мбіт/с з можливістю оперативного розширення до 10 000/10000 мбіт/с\* | до 31.12.2024 |  |  |
| 2. | Послуга з підтримки блоку ір-адрес автономної системи (AS)  | 1 автономна система | до 31.12.2024 |  |  |
| 3. | Послуги технічної підтримки та комплексного обслуговування із забезпеченням моніторингу та протидії інцидентам з інформаційної безпеки (захист від DDOS-атак)м. Київ, вул. Антоновича, будинок 51 | 1 Гбіт/с | до 31.12.2024 |  |  |
| **Вартість, грн без ПДВ** |  |
| **ПВД (20%), грн.** |  |
| **Вартість з ПДВ (20%), грн.** |  |

\*Розширення каналу до 10 000/10 000 мбіт/с повинно бути виконано Оператором за заявкою від Замовника протягом 1 (одного) календарного дня без зміни вартості Договору відповідно до Додатку  1 до Договору від \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| АБОНЕНТ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** | ОПЕРАТОР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** |

Додаток 2 до Договору
від \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

**ТЕХНІЧНІ ВИМОГИ
до послуг з надання доступу до захищеного вузла Інтернет-доступу (ЗВІД), підтримки блоку ір-адрес автономної системи (AS) та захист від DDoS-атак**

Строк надання послуг –до 31.12.2024 року.

Термін підключення послуг – не більше 1 (одного) календарного дня, з урахуванням технологічної потреби Абонента оперативного підключення до мережі Інтернет у відповідності до всіх визначених технічних вимог та для забезпечення мінімального переривання функціонування сервісів критичної інфраструктури.

**Таблиця 1.** Загальні вимоги до каналу доступу до мережі Інтернет через захищений вузол Інтернет-доступу:

| **№ з/п** | **Вимога** |
| --- | --- |
| 1 | Забезпечення послуг захищеного доступу до мережі Інтернет без обмеження трафіку через власний Захищений вузол Інтернет доступу Оператора за технологією TCP/IP по виділеним оптично-волоконним лініям зв’язку для таких сайтів Абонента:м. Київ, вул. Антоновича, будинок 51 канал зі швидкістю 3 000 Mbps з можливістю оперативного розширення каналу за вимогою Замовника до 10 000 Mbps. |
| 2 | Цілодобовий захищений доступ до мережі Інтернет повинен надаватися через власний Захищений вузол Інтернет доступу (далі – ЗВІД) Оператора, який повинен мати дійсний атестат відповідності системи захисту інформації та експертний висновок до нього, за технологією TCP/IP по виділеній оптично-волоконній лінії зв’язку. |
| 3 | 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 24.09.2001 №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 07.07.2008 за №603/15294;
* Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11.04.2012 № 295 та інших нормативно-правових актів України у сфері телекомунікацій.
 |
| 4 | Наявність власного оптоволоконного каналу зв’язку між магістральним мережним комутаційним обладнанням Абонента і Оператора. |
| 5 | Телекомунікаційна мережа, по якій надається Послуги, повинна забезпечувати безперебійну роботу Послуг. Для автономності роботи телекомунікаційна мережа має бути зарезервована додатковими засобами, що забезпечать працездатність точок взаємоз’єднання не менше 72 годин, при відключенні електроживлення, відповідно до рішення Ради національної безпеки і оборони України від 26.11.2022 року «Про забезпечення електронними комунікаційними послугами в умовах воєнного стану». |
| 6 | Безкоштовна оренда обладнання для забезпечення доступу до мережі Інтернет. |
| 7 | Час роботи в Інтернет та обсяг передачі інформації не обмежується, доступ до Інтернет 24 години на добу, транзит трафіку Абонента до Міжнародних з’єднань Оператора - не лімітований. |
| 8 | Затримка передачі даних з серверів Інтернет розташованих в Європі та США виміряна за допомогою утиліт traceroute або ping – не більш ніж 250 мілісекунд для не менш ніж 95% тестових пакетів. |
| 9 | Наявність власного високошвидкісного підключення до вузла Українського обміну трафіком UA-IX. |
| 10 | Підтримка secondary DNS на власних серверах. |
| 11 | Підтримка secondary MX на власних серверах. |
| 12 | Наявність кваліфікованої цілодобової технічної підтримки та моніторингу, надання консультативної та технічної допомоги Абоненту по забезпеченню керування доступом до ресурсів Інтернет, маршрутизації електронної пошти, поштових служб та інтерфейсу web-mail. |
| 13 | Схема підключення – по оптичному каналу зв`язку. |
| 14 | Можливість забезпечення BGP community для керування трафіком зі сторони Абонента. |
| 15 | Можливість надання послуги QoS. |
| 16 | Забезпечення доступу до статистики використання та навантаження каналу зв’язку та доступу до Інтернет. Оператор повинен мати систему централізованого моніторингу завантаженості, працездатності та інших якісних характеристик ліній електронних комунікаційних мереж, та у разі необхідності надавати ці відомості Абоненту. Оператор повинен забезпечити технічну підтримку ліній електронних комунікаційних мереж, яка включає також постійний моніторинг сталості та якості каналу електронних комунікаційних мереж, діагностику причини відхилення від заданих технічних характеристик. |
| 17 | Забезпечення адаптованого захисту на стороні Оператора каналів зв’язку між магістральним мережним комутаційним обладнанням Абонента і Оператора від паразитного мережевого трафіку, який може призвести до переповнення каналу. |
| 18 | Забезпечення налагодження мережевої фільтрації та зовнішньої маршрутизації каналів зв’язку на стороні Оператора  з метою зменшення впливу мережевих атак на функціонування інформаційних ресурсів Абонента. |
| 19 | Надання за зверненням Абонента кваліфікованої консультативної та технічної допомоги по налагодженню обладнання та сервісів Абонента, що забезпечують доступ до зовнішніх мережевих ресурсів. |
| 20 | Оператор бере на себе зобов’язання у випадку визначення його переможцем торгів забезпечити безперервність обміну даними між локальною мережею Абонента та Інтернет в період з моменту визначення переможця до моменту підписання Договору. |
| 21 | Режим надання сервісу 24х7х365. |
| 22 | Режим роботи служби експлуатації Оператора 24х7х365. |
| 23 | Максимальний час для аварійної недоступності послуг до 6 годин. |
| 24 | Повідомлення про проведення запланованої недоступності послуг за 5 робочих днів. |
| 25 | Проміжок часу для проведення запланованої недоступності послуг 23:00-06:00. |
| 26 | Загальний час проведення запланованої недоступності послуг, не більше 12 годин на місяць. |
| 27 | Загальна тривалість запланованої недоступності послуг, не більше 36 годин на рік. |
| 28 | Наявність виділення окремого телефонного номеру для підтримки сервісу SLA. |
| 29 | Пріоритизація вхідних дзвінків за виділеним номером для підтримки сервісу SLA. |
| 30 | Наявність виділення персонального співробітника служби технічної підтримки для підтримки сервісу SLA. |
| 31 | Реагування служби технічної підтримки на звернення Абонента, не пізніше 30 хв. |
| 32 | Сканування на вразливості з проведення зовнішнього та внутрішнього сканування мережевих ресурсів на наявність в них властивостей, їх ідентифікація, оцінка, кваліфікація та складання рекомендацій для їх усунення, щоквартально. |

**Таблиця 2.** Вимоги до Захищеного вузлу Інтернет доступу:

| **№ з/п** | **Вимога** |
| --- | --- |
| 1 | **Загальні вимоги** |
| 1.1 | Захищений вузол Інтернет доступу **–** повиненявляти 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 з функціональним профілем захищеності, який обов’язково має включати наступні функціональні профілі: {КА-2, КА-1, 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} або не нижче за рівнем, та рівнем гарантії оцінки коректності Г2. |
| 1.2 | 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;
* система повинна знаходитись в режимі апаратної кластеризації, територіально розмежована між двома відмовостійкими майданчиками;
* 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 порушенням безпеки від КЗЗ серверів ЗВІД;
* приймання повідомлень щодо інцидентів з порушенням безпеки від активного 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 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;
* перевірки цілісності та коректності функціонування програмних та апаратних засобів захисту (самоконтроль);
* забезпечення можливість 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;
* Оператор надає доступ до власного Приватного кабінету на вузлі ЗВІД з можливістю переглядів інцидентів інформаційної безпеки та атак, для подальшого аналізу та прийняття відповідних рішень. За запитом надається деталізована інформація про весь вхідний та вихідний трафік, в узгоджений заздалегідь, обома Сторонами, проміжок часу;
* здійснення разового налаштування вузла ЗВІД щодо блокування ресурсів, до яких обмежується доступ відповідно до рішень РНБО, що введені в дію указами Президента України;
* надання по запиту, Абонента доступу до вузла ЗВІД для самостійного керування політиками доступу для сайтів, ресурсів та додатків.
 |
| 2 | **Вимоги до операторського та технічного супроводження** |
| 2.1 | Оператор 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). |
| 2.2 | Оператор повинен надати Абоненту перелік телефонів, веб-сайт або електронну пошту (e-mail) Центру технічної підтримки протягом 2-х календарних днів з моменту підписання Договору. |
| 2.3 | Звернення (повідомлення) Абонента повинно обов’язково включати: найменування Абонента; ім'я, прізвище, контактний телефон особи, що звертається; найменування каналу на якому виникли проблеми з передачі даних; причину звернення. |
| 2.4 | На підставі звернення (повідомлення) Абонента Оператор формує заявку, що включає всі відомості, повідомлені Абонентом. |
| 2.5 | Оператор повинен здійснювати постійний моніторинг телекомунікаційних каналів зв’язку, виявлення та усунення причин відхилення від заданих технічних характеристик.Оператор повинен надавати за запитом статистичну інформацію про послуги, що надаються, за кожною точкою підключення.Оператор повинен забезпечити усунення пошкоджень телекомунікаційної мережі 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. |
| 3 | **Порядок та строки усунення інцидентів** |
| 3.1 | Відсутність надання послуг понад 0,5 години вважається інцидентом. |
| 3.2 | У випадку виникнення інцидентів Оператор негайно повідомляє про це представників технічної підтримки Абонента по телефону або через веб-сайт, або за електронною поштою (e-mail). У випадку, якщо інцидент виявлено Абонентом, останній негайно повідомляє про це представників технічної підтримки Оператора по телефону або через веб-сайт, або електронну пошту (e-mail). |
| 3.3 | Початком періоду інциденту вважається отримання Оператором від Абонента повідомлення про інцидент або повідомлення Оператором Абонента по телефону або через веб-сайт, або за електронною поштою (e-mail).Строк усунення інцидентів, які виникли з вини Оператора не повинен перевищувати 2-х годин.Порядок та строки усунення інцидентів, що виникли з вини Абонента, погоджується Сторонами в кожному окремому випадку. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг. |
| 3.4 | Про факт відновлення Послуг Оператор повідомляє Абонента по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Оператора Абонент підтверджує чи не підтверджує факт відновлення надання Послуг. |
| 3.5 | Абонент зобов’язується надавати персоналу Оператора доступ до приміщень Абонента, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Абонента, для виконання робіт по відновленню Послуг. |
| 3.6 | Для отримання необхідного доступу до приміщень Абонента, Оператор надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред’являє Абоненту службові посвідчення та направлення на виконання робіт.Абонент має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Оператора.При надходженні заявки про інцидент (відсутність Послуги з вини Оператора) 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. |

**Таблиця 3.** Загальні вимоги до захисту каналів від DDos:

| **№ з/п** | **Вимога** |
| --- | --- |
| 1 | **Загальні вимоги** |
| 1.1 | Послуги захисту Абонента від розподілених атак типу “відмова в обслуговуванні” (DDoS-атак) повинні забезпечувати доступність визначених ресурсів у випадку цілеспрямованих атак, направлених на блокування доступу легітимних користувачів внаслідок вичерпання мережних та серверних ресурсів Абонента, які розташовані на таких ресурсах Абонента:м. Київ, вул. Антоновича, будинок 51. |
| 1.2 | Послуги повинні надаватися за допомогою власного програмно-апаратного комплексу (Система захисту), що здійснює фільтрацію Інтернет-трафіку в центрі очищення Інтернет-трафіку з єдиним централізованим механізмом керування. Програмно-апаратний комплекс має належати безпосередньо Оператору. Послуга повинна надаватись Оператором з безпосереднім фізичним каналом до ресурсів Інтернет. |
| 1.3. | Система має бути реалізована із основного та резервного програмно-апаратних комплексів по захисту ресурсів, територіально розмежованих, на базі яких реалізується рішення по захисту інформаційних ресурсів в мережі Інтернет від DDoS-атак (з детальним описом роботи даних систем, схеми, функціоналу тощо). Задля забезпечення працездатності комплексу по захисту ресурсів резервний програмно-апаратний комплекс повинен бути розміщений не в місті надання Замовнику послуги каналу Інтернет – м. Київ.Принцип побудови Системи захисту, у випадку виходу з ладу одного з програмно-апаратних комплексів (основного або резервного), повинен:* забезпечити переміщення трафіку Замовника на резервний програмно-апаратний комплекс на якому буде виконана очистка трафіку, та за допомогою роутінгу повернення до захищеного сегменту вузла Замовника.

Таким чином повинна досягатись відмовостійкість системи при виходах з ладу як програмного так і апаратного забезпечення системи. Резервування програмно-апаратних комплексів підтверджується довідкою з детальними описами роботи систем та наданням схеми резервування. |
| 1.4. | Система захисту повинна забезпечувати:* захист діапазону IP-адрес закріпленої за Абонентом автономної системи (блоку провайдеро-незалежних IP-адрес) найбільш відповідальних ресурсів Системи;
* реалізацію комплексу механізмів виявлення паразитного трафіку з можливістю оперативного розширення переліку цих механізмів на вимогу Абонента та застосування наступних механізмів фільтрації:
* фільтрацію на основі “чорних і білих” списків IP-адрес, з можливістю редагування їх Абонентом у режимі on-line;
* фільтрацію за географічною ознакою (за місцем розташування джерела трафіку), як з можливістю блокування або пропуску окремих країн та регіонів з можливістю редагування їх Абонентом у режимі on-line;
* фільтрацію на основі аналізу коректності використання протоколів;
* пропуск трафіку тільки за визначеним Абонентом списком протоколів;
* фільтрацію на засадах контрзаходів, що дозволяють відокремлювати й блокувати паразитний трафік з атаками мережевого, транспортного та прикладного рівнів (L3, L4 та L7);
* віддалений доступ до веб порталу контролю параметрів роботи Системи захисту, статистики, звітів, аналізу параметрів трафіку й виявлених аномалій;
* можливість самостійного керування Абонентом власним захистом за допомогою віддаленого порталу Системи захисту – зміна параметрів захисту, зупинка та поновлення захисту тощо без залучення Оператора;
* можливість збору та збереження мережевого трафіку під час атаки для подальшого аналізу та розслідування;
* забезпечення додаткової аналітики по вимірюваному трафіку та маршрутизації трафіку глобальної мережі;
* безперервну роботу в режимі 24х7 із забезпеченням автоматичного реагування;
* відсутність обмежень у тривалості захисту при довготривалих DDoS-атаках;
* ефективне очищення асиметричного трафіку для забезпечення можливої роботи систем Абонента з декількома провайдерами доступу в Інтернет;
* автоматичні повідомлення про початок/завершення DDoS атак;
* ведення та зберігання журналів реєстрації подій протягом мінімум 1-го (одного) місяця;
* побудову звітів про роботу Системи захисту, зміну параметрів її роботи, наявності атак на захищені ресурси.
 |
| 1.5. | Інтеграція з хмарним сервісом (рівня ATLAS Intelligence Feed або аналог) для отримання в реальному часі інформації про атаки, що відбуваються в світі, і засоби захисту від них. |
| 2 | **Технічні параметри роботи Системи захисту** |
| 2.1 | Загальні параметри:* ємність отриманого очищеного трафіку через Систему захисту: 1 (один) канал 1000 Mbps
* у разі необхідності, надавач послуги повинен мати можливість застосування сервісу хмарної очистки паразитного трафіку;
* час реакції на початок атаки: до 30 секунд (при автоматичному спрацюванні системи);
* потужність Системи захисту по відбиттю L3 атак не менш ніж 100 Gbps з можливістю обробки не менш ніж 100 Mpps мережевих IP пакетів у секунду;
* потужність Системи захисту по відбиттю L4/L7 атак не менш ніж 20 Gbps з можливостю обробки не менш ніж 36 Mpps мережевих IP пакетів у секунду без обмежень на кількість одночасних сесій та нових сесій за секунду;
* відсутність потреби Системи в будь-якому створенні профілю легітимного трафіку (створення еталонної моделі поведінки трафіку) для унеможливлення залежності поведінки Системи захисту від зміни профілю трафіку;
* відсутність потреби аналізу зворотнього трафіку для ефективного захисту від DDoS-атак при роботі систем Абонента з декількома провайдерами доступу в Інтернет.Абонент має право змінювати обсяг Послуг з урахуванням вимог Закону України «Про публічні закупівлі» (зі змінами та доповненнями).
 |
| 2.2 | Гарантована функціональність у режимі очищення трафіку під час атаки:* система захисту повинна пропускати трафік від адресатів, включених Абонентом в “білий список”;
* система захисту повинна блокувати трафік від адресатів, включених Абонентом в “чорний список”;
* система захисту повинна забезпечувати можливість ведення “чорного” та “білого” списків, а також керування станом захисту;
* система захисту повинна забезпечувати можливість повної заборони та/або обмеження швидкості бітової та/або пакетної для адресатів за наступними характеристиками:
* для окремих країн (геолокація);
* для окремих мережевих протоколів;
* для окремих типів мережевих пакетів.
* система захисту повинна забезпечувати можливість обмежувати для адресатів наступні характеристики:
* кількість TCP та/або НТТР сесій;
* тривалість TCP та/або НТТР сесій;
* мінімально допустиму бітову та/або пакетну швидкість для TCP та/або НТТР сесій.
* захист від атак з використанням протоколів поза специфікацією (Invalid Packets);
* захист від нелегітимного трафіку на незатребуваний протокол та/або порт (Flood Attacks: TCP, UDP, ICMP, DNS, SSDP, NTP, SNMP, тощо);
* захист від посилених атак (Amplification Attacks: Chargen Amplification, DNS Amplification, NTP Amplification, SNMP Amplification, SSDP Amplification, тощо);
* захист від атак з використанням фрагментованих пакетів (Fragmentation Attacks: Teardrop, Targa3, Jolt2, Nestea, тощо);
* захист від атак на виснаження TCP стеку (TCP Stack Attacks: SYN, FIN, RST, SYN ACK, URG-PSH, TCP Flags, тощо);
* відмова в обслуговуванні сервісу/ресурсу атакою за протоколом HTTP шляхом відправлення даних:
* поза специфікацією протоколу;
* за специфікацією протоколу, але з використанням Slow-rate HTTP GET/POST/READ (Resource exhaustion attacks: Slowloris, Pyloris, LOIC, тощо);
* фільтрація трафіку в умовах наявності великої кількості легітимних користувачів ресурсу з генерацією трафіку з різними характеристиками;
* інші типи атак (Application Attacks: HTTP GET ﬂoods, SIP Invite ﬂoods, DNS attacks, HTTPS protocol attacks, тощо);
* для покращення рівня захисту від паразитного трафіку Система захисту має бути підключена до всесвітньо відомих баз даних DDoS атак та отримувати дані в режимі on-line щодо:
* відомих ботнет-мереж,
* репутацій IP адрес,
* сигнатур відомих атак,

та відповідно превентивно блокувати паразитний трафік, базуючись на отриманих даних. |
| 2.3 | Реагування на інциденти:* час реагування (годин, робочий час): протягом 1-2 годин після звертання (по електронній пошті або телефону).
 |
| 2.4 | Вирішення інцидентів:* час вирішення (годин, робочий час): протягом одного-двох робочих днів  після звертання.
 |
| 2.5 | Термін зберігання інформації - 1 місяць. |
| 2.6 | Надання інформації в процесі вирішення інцидентів – обов’язково. |
| 3 | **Вимоги до технічного супроводу** |
| 3.1 | Служба технічного супроводу повинна забезпечувати обробку запитів уповноважених осіб Абонента та передбачати:* приймання запитів, їх реєстрацію, класифікацію й маршрутизацію на наступні рівні підтримки;
* контроль ходу виконання робіт за запитом, прискорення у випадку виникнення проблем з виконанням запиту, інформування уповноважених осіб Абонента про хід виконання робіт, закриття запиту;
* моніторинг Оператором та Абонентом роботи системи захисту online з можливістю формування звітів про атаки;
* інформування уповноважених осіб Абонента про зміни, регламентні та технологічні роботи.

 Оператор розпочинає процес мінімізації шкоди від атаки після встановлення факту атаки засобами власної інфраструктури або отримання підтвердження Абонента через визначені в Договорі засоби зв’язку, та скеровує трафік Абонента до Системи захисту під час такої атаки. Час для мінімізації шкоди від атаки розраховується з того моменту, коли Оператор скеровує трафік до Системи захисту під час такої атаки. Відповідний рівень надання послуги щодо кожного типу Атаки наведено у таблиці:

|  |  |
| --- | --- |
| **Основні типи Атаки** | **Час, необхідний для відновлення відповідного рівня послуги** |
| UDP/ICMP Floods | 2 хвилини |
| SYN Floods | 10 хвилин |
| TCP Flag Abuses | 2 хвилини |
| DNS Reflection | 20 хвилин |
| DNS Attack | 20 хвилин |

 |

**Таблиця 4:** Вимоги до операторського та технічного супроводження:

| **№ з/п** | **Вимога** |
| --- | --- |
| 1 | **Загальні вимоги** |
| 1.1 | Оператор 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). |
| 1.2 | Оператор повинен надати Абоненту перелік телефонів, веб-сайт або електронну пошту (e-mail) Центру технічної підтримки протягом 2-х календарних днів з моменту підписання Договору. |
| 1.3 | Звернення (повідомлення) Абонента повинно обов’язково включати: найменування Абонента; ім'я, прізвище, контактний телефон особи, що звертається; найменування каналу на якому виникли проблеми з передачі даних; причину звернення. |
| 1.4 | На підставі звернення (повідомлення) Абонента Оператор формує заявку, що включає всі відомості, повідомлені Абонентом. |
| 1.5 | Оператор повинен здійснювати постійний моніторинг послуг задля виявлення та усунення причин відхилення від заданих технічних характеристик.Оператор повинен надавати за запитом статистичну інформацію про послузі, що надається. |
| 2 | **Порядок та строки усунення інцидентів** |
| 2.1 | Відсутність надання послуг понад 0,5 години вважається інцидентом. |
| 2.2 | У випадку виникнення інцидентів Оператор негайно повідомляє про це представників технічної підтримки Абонента по телефону або через веб-сайт, або за електронною поштою (e-mail). У випадку, якщо інцидент виявлено Абонентом, останній негайно повідомляє про це представників технічної підтримки Оператора по телефону або через веб-сайт, або електронну пошту (e-mail). |
| 2.3 | Початком періоду інциденту вважається отримання Оператором від Абонента повідомлення про інцидент або повідомлення Оператором Абонента по телефону або через веб-сайт, або за електронною поштою (e-mail).Строк усунення інцидентів, які виникли з вини Оператора не повинен перевищувати 2-х годин.Порядок та строки усунення інцидентів, що виникли з вини Абонента, погоджується Сторонами в кожному окремому випадку. Завершенням періоду інциденту вважається час фактичного усунення інциденту та відновлення Послуг. |
| 2.4 | Про факт відновлення Послуг Оператор повідомляє Абонента по телефону та дублює повідомлення через веб-сайт або електронну пошту (e-mail). На повідомлення Оператора Абонент підтверджує чи не підтверджує факт відновлення надання Послуг. |
| 2.5 | Абонент зобов’язується надавати персоналу Оператора доступ до приміщень Абонента, необхідного телекомунікаційного обладнання, що забезпечує надання Послуг та розміщене в приміщеннях Абонента, для виконання робіт по відновленню Послуг. |
| 2.6 | Для отримання необхідного доступу до приміщень Абонента, Оператор надсилає листа з переліком працівників, які будуть виконувати роботи. Оператор пред’являє Абоненту службові посвідчення та направлення на виконання робіт.Абонент має право отримувати інформацію про хід виконання робіт по відновленню Послуг шляхом звернення до представників технічної підтримки Оператора.При надходженні заявки про інцидент (відсутність Послуги з вини Оператора) 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. |

|  |  |
| --- | --- |
| АБОНЕНТ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** | ОПЕРАТОР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** |

Додаток 3 до Договору
від \_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

**ВІДПОВІДАЛЬНІ ПРЕДСТАВНИКИ СТОРІН**

1. **Відповідальні представники Оператора**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Питання** | **Прізвище, Ім’я, По-батькові** | **Телефон** | **Адреса електронної пошти** |
| 1 | Технічні/Аварійні | Черговий зміни |  |  |
| 2 | Бухгалтерія |  |  |  |
| 3 | Загальні |  |  |  |

1. **Відповідальні представники Абонента**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Питання** | **Прізвище, Ім’я, По-батькові** | **Телефон** | **Адреса електронної пошти** |
| 1 | Адміністративні |  |  |  |
| 2 | Бухгалтерія |  |  |  |
| 3 | Технічні |  |  |  |

|  |  |
| --- | --- |
| АБОНЕНТ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** | ОПЕРАТОР:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_****м.п.** |