ТОВ «ЮАСІТІ»

ПРАВИЛА ДОПУСТИМОГО КОРИСТУВАННЯ ПОСЛУГАМИ (AUP)

для бізнес-клієнтів, юридичних осіб та фізичних осіб – підприємців

Документ	ПРАВИЛА ДОПУСТИМОГО КОРИСТУВАННЯ ПОСЛУГАМИ (AUP)
Версія	1.0
Статус	Шаблон для розміщення на сайті
Чинно з	20.03.2026
Для кого	Бізнес-клієнти / юридичні особи / ФОП

Розміщення на сайті Провайдера
Провайдер: ТОВ «ЮАСІТІ» Код ЄДРПОУ 35745743 Номер у Реєстрі постачальників електронних комунікаційних мереж та послуг: 1868
Сайт: https://biz.uacity.net/legal/
Контакт з договірних питань: info@uacity.net, 0 (800) 600 300
Контакт технічної підтримки: noc@uacity.net, 0 (800) 600 300, 24/7

1. Призначення та сфера дії

1.1. Ці Правила допустимого користування послугами (Acceptable Use Policy, AUP) визначають допустимі та заборонені способи використання мережі, обладнання та послуг Провайдера.

1.2. AUP застосовується до всіх послуг Провайдера, що надаються бізнес-клієнтам, у тому числі до доступу до Інтернету, каналів передачі даних, додаткових IP-сервісів, керованого обладнання, Wi-Fi-сервісів, серверних і супутніх рішень.

1.3. Якщо у Замовленні/Специфікації погоджений спеціальний сценарій використання (наприклад, гостьовий Wi-Fi, робота власного маршрутизатора, публічний серверний сервіс, BGP або L2/L3-інтеграція), такий погоджений сценарій має пріоритет над загальними обмеженнями AUP у відповідній частині.

2. Загальні принципи користування

2.1. Замовник використовує послуги лише у законних цілях, з дотриманням договору, цих Правил, вимог інформаційної безпеки та прав третіх осіб.

2.2. Замовник відповідає за дії своїх працівників, підрядників, орендарів, користувачів внутрішньої мережі, гостьових сегментів, Wi-Fi-мереж та пристроїв, що отримують доступ до мережі через послугу Провайдера.

2.3. Замовник повинен вживати розумних заходів безпеки: використовувати складні паролі, актуальні оновлення, антивірусний захист, резервування конфігурацій, захист від несанкціонованого доступу та обмеження публічних сервісів за потреби.

3. Заборонені дії

3.1. Забороняється використовувати послуги Провайдера для діяльності, що порушує законодавство України або права третіх осіб, зокрема для незаконного доступу до інформаційних систем, розповсюдження шкідливого програмного забезпечення, шахрайства, підробки трафіку, фішингу, незаконного збору персональних даних чи інших протиправних дій.

3.2. Забороняється створювати, розсилати або ретранслювати масові небажані повідомлення (spam), керувати open relay/open proxy, підміняти заголовки листів, приховувати джерело шкідливого трафіку або обходити обмеження, встановлені Провайдером чи законом.

3.3. Забороняється проводити DDoS/DoS-атаки, сканування портів з ознаками зловживання, брутфорс, використання ботнетів, генерацію аномального трафіку, умисне перевантаження мережевих вузлів, серверів або систем третіх осіб.

3.4. Забороняється несанкціоновано втручатися в мережу Провайдера, підключати неузгоджене активне обладнання до інфраструктури Провайдера, розкривати або змінювати опломбовані елементи, підміняти MAC/ідентифікатори там, де це прямо заборонено конфігурацією сервісу.

3.5. Забороняється перепродавати, субліцензувати, реекспортувати або передавати послугу третім особам як окрему публічну електронну комунікаційну послугу без прямої письмової згоди Провайдера.

4. Публічні сервіси, сервери та мережеві сервіси Замовника

4.1. Використання публічних серверів, VPN-шлюзів, VoIP-вузлів, відеоспостереження, зовнішніх веб-сервісів, поштових сервісів та інших сервісів з підвищеним ризиком навантаження або безпеки допускається лише за умови, що це не порушує закон, не створює загрози мережі і відповідає погодженим технічним параметрам послуги.

4.2. Провайдер може вимагати від Замовника технічних заходів для мінімізації ризиків: фільтрації, rate limiting, ACL, захисту поштових серверів, закриття open services, блокування заражених хостів або тимчасового обмеження окремих портів/протоколів.

4.3. Якщо Замовнику потрібні підвищені ліміти, незвична модель трафіку, BGP, публічні сервери з істотним навантаженням, анонсування префіксів чи інші нестандартні умови, вони мають бути погоджені окремо в Замовленні/Специфікації.

5. Зловживання трафіком та інформаційна безпека

5.1. Ознаками зловживання можуть вважатися: аномально високий обсяг вихідного трафіку, різкі піки PPS/BPS, масові однотипні з’єднання, часті звернення до великої кількості зовнішніх адрес, ознаки участі у ботнет-активності, масові SYN/UDP-флуди, а також підтверджені звернення від інших операторів, CERT, провайдерів хмарних сервісів або державних органів.

5.2. Замовник зобов’язаний невідкладно реагувати на повідомлення Провайдера про зараження, компрометацію або використання мережі не за призначенням та вживати заходів для усунення порушення.

5.3. До усунення загрози Провайдер має право застосувати пропорційні запобіжні заходи: тимчасово обмежити окремі напрямки трафіку, швидкість, конкретні сервіси, порти, IP-адреси або повністю призупинити послугу, якщо це необхідно для захисту мережі чи третіх осіб.

6. Реагування на порушення AUP

6.1. Залежно від характеру порушення Провайдер може: (а) направити попередження; (б) вимагати усунення порушення у визначений строк; (в) тимчасово обмежити окремий сервіс, порт, VLAN, IP або сесію; (г) тимчасово призупинити надання послуги; (ґ) ініціювати дострокове припинення відповідної послуги або договору у разі істотного чи повторного порушення.

6.2. Якщо зволікання створює реальну загрозу мережі, даним третіх осіб або стабільності послуг, Провайдер може застосувати технічні обмеження негайно, з подальшим повідомленням Замовника у розумний строк.

6.3. Усунення наслідків порушення, додаткові виїзди, аналіз інциденту або відновлення сервісу можуть оплачуватися відповідно до Прайсу, якщо це прямо передбачено договором або рахунком.

7. Повідомлення про інциденти та співпраця Замовника

7.1. Замовник зобов’язаний негайно повідомляти Провайдера про відомі інциденти безпеки, втрату контролю над обладнанням, компрометацію облікових даних, а також про звернення третіх осіб чи державних органів, що прямо стосуються користування послугою.

7.2. На запит Провайдера Замовник надає мінімально необхідну технічну інформацію, що допоможе локалізувати інцидент: IP-адреси, часові інтервали, тип сервісу, характер трафіку, логи, контакт відповідальної особи.

7.3. Замовник не повинен самостійно виконувати дії на стороні мережі Провайдера або давати вказівки третім особам втручатися в мережу Провайдера без його згоди.

8. Заключні положення

8.1. Це AUP є невід’ємною частиною договірного пакета документів Провайдера і застосовується разом із рамковим договором, Замовленнями/Специфікаціями, Стандартними умовами, SLA та Прайсом.

8.2. Провайдер розміщує на сайті чинну редакцію AUP та архів попередніх редакцій. Для діючих послуг нова редакція застосовується у порядку, передбаченому рамковим договором або Стандартними умовами.

8.3. У всьому, що не врегульовано цим документом, Сторони керуються договором та законодавством України.