ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2023 року № ____

ПРИМІРНА ПУБЛІЧНА ПРОПОЗИЦІЯ

про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

_____
(найменування/прізвище, власне ім'я, по батькові (за наявності) Власника системи)
(далі – Власник системи), в особі _____,
(посада, прізвище, власне ім'я, по батькові (за наявності))
що діє на підставі _____,
(статут, положення, довіреність/паспорт)
та _____
(найменування/прізвище, власне ім'я, по батькові (за наявності) Координатора)
(далі – Координатор), в особі _____,
(посада, прізвище, власне ім'я, по батькові (за наявності))
що діє на підставі _____,
(статут, положення, довіреність/паспорт)
(у разі залучення Координатора), з однієї сторони, пропонують необмеженому колу фізичних або юридичних осіб (далі – Дослідник), крім випадків визначених пунктом 29 цієї Публічної пропозиції, з іншої сторони (далі разом – Сторони, а кожна окремо – Сторона), здійснити пошук та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – системи) Власника системи.

Ця Публічна пропозиція укладається відповідно до статті 634 Цивільного кодексу України та пункту 4 Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 року № 497 (далі – Порядок), її умови однакові для всіх Дослідників.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Ця Публічна пропозиція оприлюднена на власному офіційному вебсайті _____
(Власника системи або Координатора (у разі залучення Координатора))

за адресою _____.
(адреса мережі Інтернет, на якій оприлюднено Публічну пропозицію)

2. У цій Публічній пропозиції терміни вживаються у значенні, наведеному у Законах України "Про основні засади забезпечення кібербезпеки України", "Про електронні комунікації", "Про захист інформації в інформаційно-комунікаційних системах", Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, а також у Порядку.

3. У разі зміни, доповнення цієї Публічної пропозиції або припинення її дії _____
(Власник системи або Координатор (у разі залучення Координатора))
готує відповідне повідомлення та завчасно, не пізніше ніж за _____ днів
(кількість)
оприлюднює його на власному офіційному вебсайті.

4. Дослідник для пошуку та виявлення потенційної вразливості систем приймає всі умови цієї Публічної пропозиції без будь-яких винятків та/або обмежень, що вважається приєднанням (акцептом) до цієї Публічної пропозиції.

Направленням звіту про вразливість системи за результатами пошуку її потенційної вразливості (далі – звіт) Дослідник підтверджує беззаперечну згоду з умовами цієї Публічної пропозиції, підтверджує повну відповідність вимогам, що висуваються до Дослідника, та висловлює готовність виконувати її умови повною мірою.

При приєднанні до цієї Публічної пропозиції Дослідник надає згоду (для фізичних осіб) _____
(Власнику системи та Координатору (у разі залучення Координатора))
на збір, використання та обробку персональних даних, а також вчиняти дії, передбачені Законом України «Про захист персональних даних».

ПРЕДМЕТ ПУБЛІЧНОЇ ПРОПОЗИЦІЇ

5. Здійснення пошуку та виявлення потенційної вразливості системи є вільною та добровільною дією. Дослідник не має отримувати будь-які попередні дозволи та погодження при умові дотримання вимог цієї Публічної пропозиції та Порядку.

Відповідно до частини шостої статті 361 Кримінального кодексу України дії Дослідника, вчинені відповідно до Порядку, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

6. Ця Публічна пропозиція поширюється на:

_____
(опис системи (назва системи, її версія та інша інформація, яка дає можливість визначити систему))

_____
(адреса мережі Інтернет/адресний простір мережі Інтернет, домен, IP-адреса)

_____.
(інше)

7. Ця Публічна пропозиція не поширюється на:

_____
(адреса мережі Інтернет/адресний простір мережі Інтернет, домен, IP-адреса)

_____
(адреса мережі Інтернет/адресний простір мережі Інтернет, домен, IP-адреса)

_____.
(інше)

8. Досліднику заборонено:

використовувати вразливість для отримання вигоди, заподіяння втрат, дослідження інших систем, отримання персональних даних;

здійснювати збір інформації про користувачів системи за допомогою методів соціальної інженерії;

здійснювати розподілені атаки на відмови в обслуговуванні (DoS, DDoS), а також використовувати системи автоматичного тестування, які генерують масивні об'єми мережевого трафіка та можуть вплинути на стале функціонування системи;

_____.
(інше)

ПОРЯДОК НАДАННЯ ЗВІТУ, ВИМОГИ ДО ЙОГО ПІДГОТОВКИ ТА ФОРМИ

9. Дослідник, знайшовши потенційну вразливість системи, повідомляє

_____
(Власника системи або Координатора (у разі залучення Координатора))

про виявлену вразливість та надає звіт _____
(опис механізму інформування,

_____.
електронна адреса, посилання на форму тощо)

10. Звіт оформляється у довільній формі та повинен містити таку інформацію:

інформація про Дослідника (прізвище, власне ім'я, електронна адреса та/або мобільний телефон, або інший контакт для можливості подальшої комунікації);

система, в якій виявлено вразливість, місце виявлення вразливості: сервіс, адреса мережі Інтернет тощо;

назва вразливості, опис впливу вразливості на функціональність та безпеку системи, суб'єктивна оцінка та пояснення рівня ризику вразливості;

докази існування вразливості: текстовий опис кроків відтворення (використання) вразливості, трафік або здійснення клієнт-серверного

інтернет-протоколу (HTTP сесії), знімки екрана та/або відео або код перевірки концепції існування вразливості (Proof of Concept (PoC) код);

_____.
(інша інформація)

11. Дослідник може надати додаткову інформацію про вразливість, яка може знадобитися для її виправлення.

12. _____
(Власник системи або Координатор (у разі залучення Координатора))
найбільше зацікавлений в отриманні звіту щодо таких вразливостей:

_____.
(перелік вразливостей)

ПРАВА ТА ОБОВ'ЯЗКИ СТОРІН

13. Уся інформація, отримана в рамках здійснення пошуку та виявлення потенційної вразливості системи, належить_____
(Власнику системи та Координатору (у разі залучення Координатора))
та вважається конфіденційною. Дослідник зобов'язаний дотримуватися вимог законодавства щодо конфіденційної інформації.

_____
(Власник системи та Координатор (у разі залучення Координатора))
може використовувати, оприлюднювати або іншим чином розповсюджувати інформацію про виявлену вразливість.

14. Період нерозголошення інформації про вразливість системи становить _____ з дати реєстрації звіту.
(період (не більше ніж шість місяців))

15. Власник системи має право:

відмовити Досліднику в подальшому опрацюванні звіту, якщо звіт не відповідає вимогам, визначеним в пункті 10 цієї Публічної пропозиції, та/або якщо у звіті зазначено інформацію про вразливість системи, виявлену раніше іншим Дослідником;

прийняти рішення про не внесення змін до системи за результатами перевірки звіту;

змінювати, доповнювати Публічну пропозицію або припиняти її дію;

прийняти рішення про оприлюднення інформаціїї про виявлену вразливість до внесення змін до системи.

16. Власник системи має право (у разі залучення Координатора):

прийняти рішення про не внесення змін до системи за результатами перевірки звіту;

погодитися на пропозицію Координатора або прийняти рішення щодо внесення змін до Публічної пропозиції або припинення її дії;

прийняти рішення про оприлюднення інформаціїї про виявлену вразливість до внесення змін до системи.

17. Власник системи зобов’язаний:

після отримання звіту протягом 10 робочих днів зареєструвати його та повідомити Дослідника про те, що звіт отримано, зазначивши реєстраційний номер та дату реєстрації звіту;

перевірити отриманий звіт на відповідність вимогам, визначеним у пункті 10 цієї Публічної пропозиції, на предмет наявності в ньому інформації про вразливість системи, виявлену раніше іншим Дослідником;

повідомити Дослідника про відмову в подальшому опрацюванні звіту, якщо звіт не відповідає вимогам, визначеним в пункті 10 цієї Публічної пропозиції, та/або якщо у звіті заначено інформацію про вразливість системи, виявлену раніше іншими дослідниками, зазначивши реєстраційний номер та дату такого звіту;

після перевірки звіту протягом 30 робочих днів з дати реєстрації звіту повідомити Дослідника про прийняте рішення щодо внесення або не внесення змін до системи;

під час вжиття заходів щодо внесення змін до системи підготувати та оприлюднити на власному офіційному вебсайті інформацію про виявлення вразливості та внесення змін до системи;

після перевірки звіту у разі прийняття рішення щодо внесення змін до системи виплатити/надати винагороду та/або публічно висловити подяку Досліднику відповідно до вимог пунктів 26 і 27 цієї Публічної пропозиції.

18. Власник системи зобов’язаний (у разі залучення Координатора) після перевірки звіту протягом 30 робочих днів з дати реєстрації звіту повідомити Координатора про прийняте рішення щодо внесення або не внесення змін до системи.

19. Дослідник має право:

здійснювати пошук та виявлення вразливості системи (складової системи), яка визначена в пункті 6 цієї Публічної пропозиції, методами, визначеними пунктом 7 Порядку;

здійснювати збір доказів наявності вразливості для формування звіту, виконуючи лише такі дії, що є необхідними для отримання доказів наявності вразливості;

після перевірки звіту у разі прийняття рішення Власником системи щодо внесення змін до системи отримати винагороду за виявлену вразливість та/або публічно висловлену подяку відповідно до вимог пунктів 26 і 27 цієї Публічної пропозиції;

не погодитися на публічне висловлювання подяки, _____,

(Власником системи або Координатором (у разі залучення Координатора))

в якому зазначається його власне ім’я та прізвище або псевдонім;

оприлюднити інформацію про виявлену вразливість та її технічні особливості у разі отримання від _____
(Власника системи або Координатора (у разі залучення Координатора))
повідомлення про не внесення змін до системи або після закінчення терміну, визначеного пунктом 14 цієї Публічної пропозиції.

20. Дослідник зобов'язаний:

не виконувати дії щодо системи (складової системи), які визначені в пункті 8 цієї Публічної пропозиції;

після завершення пошуку потенційної вразливості системи повідомити про результати та надати звіт _____
(Власнику системи або Координатору (у разі залучення Координатора))
відповідно до вимог пункту 10 цієї Публічної пропозиції;

не розголошувати інформацію про виявлену вразливість до завершення періоду визначеного пунктом 14 цієї Публічної пропозиції;

при взаємодії з _____
(Власником системи або Координатором (у разі залучення Координатора))
використовувати лише власні персональні дані (фізичних осіб) та дані юридичної особи відповідно до Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань;

підписати акти виконаних робіт щодо виявлених вразливостей та іншу необхідну документацію, яка може знадобитися _____.
(Власнику системи або Координатору (у разі залучення Координатора))

21. Координатор має право (у разі залучення Координатора):

відмовити Досліднику в подальшому опрацюванні звіту, якщо звіт не відповідає вимогам, визначеним в пункті 12 цієї Публічної пропозиції, та/або якщо у звіті зазначено інформацію про вразливість системи, виявлену раніше іншим Дослідником;

змінювати, доповнювати Публічну пропозицію або припиняти її дію за рішенням та/або згодою Власника системи.

22. Координатор зобов'язаний (у разі залучення Координатора):

після отримання звіту протягом 10 робочих днів зареєструвати його та повідомити Дослідника про те, що звіт отримано, зазначивши реєстраційний номер та дату реєстрації звіту;

перевірити отриманий звіт на відповідність вимогам, визначеним в пункті 10 цієї Публічної пропозиції, на предмет наявності в ньому інформації про вразливість системи, виявлену раніше іншим Дослідником;

повідомити Дослідника про відмову в подальшому опрацюванні звіту, якщо звіт не відповідає вимогам, визначеним в пункті 10 цієї Публічної пропозиції, та/або якщо у звіті заначено інформацію про вразливість системи, виявлену раніше іншими дослідниками, зазначивши реєстраційний номер та дату такого звіту;

повідомити Власника системи про отриманий звіт і результати його перевірки;

після перевірки звіту протягом 30 робочих днів з дати реєстрації звіту повідомити Дослідника про прийняте рішення Власника системи щодо внесення або не внесення змін до системи;

під час вжиття заходів щодо внесення змін до системи підготувати та оприлюднити інформацію про виявлення вразливості та внесення змін до системи;

за рішенням Власника системи оприлюднити інформацію про виявлену вразливість до внесення змін до системи;

після перевірки звіту у разі прийняття рішення Власником системи щодо внесення змін до системи виплатити/надати винагороду та/або публічно висловити подяку Досліднику відповідно до вимог пунктів 26 і 27 цієї Публічної пропозиції.

ВИНАГОРОДА

23. Винагорода Досліднику встановлюється відповідно до рівня складності (критичності) виявленої вразливості системи/винагорода Досліднику за виявлену вразливість не передбачається (вибрати варіант).

24. Під винагородою слід розуміти _____
(опис винагороди)
залежно від категорії вразливості, що наведена в таблиці.

Категорія вразливостей	Вразливості	Винагорода

25. _____
(Власник системи або Координатор (у разі залучення Координатора))
визначає категорію вразливості. Категорія вразливості визначається за допомогою _____.
(спосіб визначення категорії вразливості)

26. Виплата/надання винагороди Досліднику здійснюється _____
(Власником системи або Координатором (у разі залучення Координатора))
у разі прийняття Власником системи рішення про внесення змін до системи та здійснюється протягом 10 робочих днів після оприлюднення _____
(Власником системи або Координатором (у разі залучення Координатора))
інформації про виявлення вразливості та внесення змін до системи.

27. За згодою Дослідника _____
(Власник системи або Координатор (у разі залучення Координатора))
може опублікувати на власному офіційному вебсайті повідомлення з

висловленням подяки Досліднику, в якому зазначається власне ім’я та прізвище або псевдонім Дослідника, незалежно від того, чи є звіт Дослідника повторенням інформації про вразливість системи, виявлену раніше іншими дослідниками, або якщо за знайдення вразливості за звітом цією Публічною пропозицією не передбачена виплата винагороди.

28. Винагорода не здійснюється:

_____

(опис випадків, у разі яких не здійснюється винагорода)

_____

(перелік вразливостей, за які не здійснюється винагорода

_____.

(інше)

ІНШІ ПОЛОЖЕННЯ

29. Здійснювати пошук та виявлення потенційної вразливості систем не можуть фізичні та/або юридичні особи:

які брали участь у будь-якій частині розробки, адміністрування та/або виконання цієї Публічної пропозиції;

які є працівниками та були працівниками протягом останніх шести місяців та/або надавали послуги Власнику системи, а також пов'язані з розробкою, адмініструванням, підтримкою системи;

члени сім'ї або пов'язані особи з будь-ким, про кого зазначено в абзацах другому та третьому цього пункту;

працівники підприємств, установ, організацій будь-якої форми власності, політика яких забороняє без надання дозволу роботодавця, брати участь в публічних пропозиціях такого виду;

особи, з якими відповідно до законодавства України обмежені чи заборонені банківські безготівкові розрахунки;

щодо яких застосовані санкції відповідно до Закону України “Про санкції”;

які створені та зареєстровані відповідно до законодавства держави, визнаної Верховною Радою України державою-агресором, та/або держав, які входять до митних та воєнних союзів з такою державою, та/або щодо яких застосовано санкції відповідно до Закону України “Про санкції” і щодо яких прийнято рішення про застосування санкцій в Україні;

які створені та зареєстровані відповідно до законодавства України кінцевим бенефіціарним власником, учасником (акціонером) або членом яких є держава-агресор, громадянин держави-агресора або юридична особа, створена та зареєстрована відповідно до законодавства держави-агресора та/або держав, які входять до митних і воєнних союзів з такою державою та/або щодо яких застосовані санкції відповідно до Закону України “Про санкції”;

_____.

(інше)

30. Дослідник несе персональну відповідальність за сплату всіх податків та обов'язкових платежів у разі отримання винагороди, пов'язаних з цією Публічною пропозицією.

31. Надіславши звіт Дослідник відповідно до законодавства передає Власнику системи всі права інтелектуальної власності на інформацію зазначену в звіті.

32. Якщо ви як Дослідник не погоджуєтесь з будь-якими умовами цієї Публічної пропозиції, будь ласка, не надсилайте звіт та будь-які інші повідомлення щодо здійснення пошуку та виявлення потенційної вразливості системи.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку
полковник Данило МЯЛКОВСЬКИЙ