**РЕГЛАМЕНТ взаємодії сторін в процесі фільтрації фішингових доменів**

**(проект)**

**1. Загальні положення.**

Цей Регламент описує основні принципи та процедури взаємодії учасників Системи фільтрації фішингових доменів.

Метою співробітництва сторін є захист від фішингу банків та їх користувачів, які одночасно є абонентами операторів електронних комунікацій.

Система фільтрації фішингових доменів не застосовується для фільтрації доменів та обмеження доступу до інтернет-ресурсів, які використовуються для поширення шкідливого програмного забезпечення, пропаганди, дезінформації тощо, а також до інтернет-ресурсів, обмеження доступу до яких здійснюється відповідно до Закону України «Про санкції».

**2. Терміни та визначення.**

У цьому документі наведені нижче терміни вживаються в такому значенні:

Фішинг – незаконне заволодіння реквізитами платіжних інструментів інтернет-користувачів та інформацією, необхідною для входу до банківських систем дистанційного обслуговування;

CSIRT-NBU – команда реагування на кіберінциденти в банківській системі України (визначена ст. 2 Положення про організацію кіберзахисту в банківській системі України, затвердженого Постановою Правління НБУ від 12.08.2022 р. № 178);

надавач сервісу DNS (далі - Провайдер) – провідний постачальник електронних комунікаційних мереж та/або послуг, який надає кінцевому користувачу (пов’язану) послугу з отримання інформації про домени (DNS);

учасники Системи – CSIRT-NBU та Провайдери;

система фільтрації фішингових доменів (далі – Система) – механізм взаємодії CSIRT-NBU і Провайдерів для протидії фішингу;

лендінгова сторінка – інтернет-сторінка Провайдера, на яку здійснюється перенаправлення запитів кінцевого користувача на домени з переліку фішингових доменів, яка містить інформацію про причини такого перенаправлення;

DNS - комп’ютерна розподілена система для отримання інформації про домени;

API – набір визначених методів для запиту даних, аналізу, обробки та надсилання відповіді на запити;

Інші терміни у цьому документі вживаються у значеннях, визначених законодавством України.

**3. Принципи фільтрації доменів.**

Одним із поширених видів шахрайства в інтернет є створення фішингових ресурсів, які мають на меті збір персональних даних громадян та інформації про банківські картки. Зловмисники реєструють фішингові домени та розміщують на них інтернет-сторінки, що імітують офіційні веб-ресурси банківських і фінансових установ, державних та міжнародних організацій, які надають фінансову допомогу або інші послуги громадянам, інтернет-магазинів тощо. Інформація, яку вводять громадяни на таких фішингових інтернет- сторінках, в подальшому використовується зловмисниками з метою викрадення коштів та в інших шахрайських схемах. Система фільтрації фішингових доменів дозволяє захистити користувачів інтернет від подібного шахрайства шляхом перенаправлення їх з фішингового домену на безпечну лендінгову сторінку.

*Основні засади функціонування Системи:*

1. Використання стандартизованого механізму API для отримування списку фішингових доменів для подальшого контролю та включення до блокування.

2. Процес фільтрації Провайдером фішингового домену відбувається у період з моменту його виявлення до видалення (призупинення дії) домену на рівні реєстратора доменних імен.

3. Фільтрація відбувається на рівні рекурсивних DNS серверів українських постачальників електронних комунікаційних послуг.

4. З метою підвищення обізнаності користувачів інтернет використовуються безпечні лендінгові сторінки, на які здійснюється перенаправлення запитів до фішингових ресурсів. Ці сторінки розміщуються на ресурсах Провайдерів та забезпечують інформування користувачів про потенційний ризик, а також механізм зворотного зв'язку.

5. Для обліку доменів та централізованого зберігання використовується окрема подія платформи MISP, для систематизації переліку фішингових доменів використовується необхідний набір тегів.

6. Провайдери регулярно відправляють запити на оновлення списків. З моменту внесення змін до переліку фішингових доменів оновлення буде доступно з наступним їх запитом. Рекомендована частота відправки запитів в робочий час – 15 хв.

7. Провайдер отримує список фішингових доменів, перевіряє та використовує механізм блокування для сайтів, які визнані фішинговими. Про домени, які не визнані ним фішинговими, Провайдер повідомляє CSIRT-NBU.

*Основні компоненти Системи:*

1. Платформа MISP (адреса публікації https://misp.bank.gov.ua/)

Платформа MISP забезпечує доступ учасників Системи до актуального переліку фішингових доменів. Перелік фішингових доменів надсилається до надавача послуг DNS із MISP-NBU (визначеного п. 11 Положення про організацію кіберзахисту в банківській системі України, затвердженого Постановою Правління НБУ від 12.08.2022 р. № 178) для подальшої обробки та прийняття рішення щодо блокування. Учасники Системи можуть використовувати платформу MISP для надання пропозицій до переліку фішингових доменів.

Будь-які транзитні сервери не можуть використовуватись у Системі задля уникнення можливості компрометації інформації.

2. Лендінгова сторінка

Інтернет-сторінка Провайдера, на яку здійснюється перенаправлення запитів кінцевого користувача на домени з переліку фішингових доменів. Вимоги до лендінгової сторінки встановлені у розділі 8.

**4. Організація взаємодії з Системою.**

Для отримання доступу до Системи Провайдер здійснює реєстрацію в Системі шляхом надсилання заявки на електронну адресу MISP-NBU вказати електронну адресу MISP-NBU

Заявка Провайдера на реєстрацію в Системі повинна містити: назву Провайдера та код ЄДПРОУ/ІПН, ПІБ та адресу електронної пошти уповноваженої особи, IP адресу(-и) серверу з якого надходитимуть запити.

Відповідно до наданих Провайдером в заявці на реєстрацію даних в платформі MISP за електронною адресою MISP-NBU вказати електронну адресу MISP-NBU створюється користувач з правами "org admin", який має права створювати додаткових користувачів з представників своєї організації.

Учасники Системи відповідають за підтримку реєстраційних даних в актуальному стані.

Після реєстрації Провайдер налаштовує на власному DNS сервері взаємодію для отримання списку блокувань.

**5. Внесення доменів до списку блокувань.**

Ведення переліку фішингових доменів покладається на галузеву команду реагування на CSIRT-NBU. Для зберігання та розповсюдження переліку фішингових доменів використовується платформа MISP-NBU.

Команда CSIRT-NBU розглядає звернення від основних суб'єктів забезпечення кібербезпеки України, визначених Законом України «Про основні засади забезпечення кібербезпеки», та Провайдерів щодо внесення доменів до переліку фішингових доменів для фільтрації. Команда CSIRT-NBU проводить періодичний перегляд статусів доменів із метою мінімізації переліку. Фільтрації підлягають тільки активні домени, не заблоковані реєстраторами доменних імен.

Команда CSIRT-NBU відповідальна за своєчасне формування, а також повноту і достовірність даних у переліку фішингових доменів, а також за ідентифікацію посадових осіб, які внесли до системи конкретний домен.

Перелік фішингових доменів затверджується за допомогою кваліфікованого електронного підпису керівника Команди CSIRT-NBU чи іншої уповноваженої ним особи.

Пропозиції щодо внесення доменів до списку блокувань здійснюються шляхом відправлення відповідного API-запиту та/або надаються на електронну адресу MISP-NBU вказати електронну адресу MISP-NBU

Пропозиції щодо внесення доменів до списку блокувань розглядаються протягом робочого часу. Строк обробки пропозиції – дві години з часу надання пропозиції.

**6. Вилучення доменів із списку блокувань.**

Пропозиції щодо вилучення доменів із списку блокувань можуть надаватися учасниками Системи та суб'єктами забезпечення кібербезпеки України, визначеними Законом України «Про основні засади забезпечення кібербезпеки». Остаточне рішення про вилучення доменів приймає CSIRT-NBU.

Пропозиції щодо вилучення доменів із списку блокувань здійснюються шляхом відправлення відповідного API-запиту та/або надаються на електронну адресою MISP-NBU вказати електронну адресу MISP-NBU.

Власник або адміністратор домену, який вважає, що його домен помилково внесено до списку блокувань, надсилає мотивовану заявку на виключення домену на електронну адресу, вказану на лендінговій сторінці. Заявка повинна містити ідентифікацію особи та підтвердженням права власності на домен.

Пропозиції щодо вилучення домену із списку блокувань мають бути розглянути протягом 6 годин у робочий час. Строк оновлення списку блокувань повинен складати до 15 хвилин з моменту внесення змін до переліку доменів.

**7. Білі списки доменів** .

За учасниками Системи, а також за суб'єктами забезпечення кібербезпеки України, визначеними Законом України «Про основні засади забезпечення кібербезпеки», залишається право надати внесення доменів до білого списку.

**8. Вимоги до лендінгової сторінки Провайдера.**

Лендінгова сторінка повинна містити:

- попередження користувачу інтернет про небезпеку переходу на фішинговий ресурс;
- доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід;
- поточну дату та час;

- адресу електронної пошти для подання заявки на виключення домену із списку блокувань.

Додатково лендінгова сторінка може містити рекомендації з кібербезпеки для користувачів інтернет.

**9. Статистика та звітність.**

При переході на лендінгову сторінку зберігається технічна інформація, що включає дату і час, доменне ім’я або URL фішингової сторінки, на яку здійснюється перехід. Термін зберігання такої інформації один тиждень.

Провайдер надає до CSIRT-NBU статистичну інформацію щодо переходів на лендінгову сторінку в порядку, визначеному Командою CSIRT-NBU. Зазначена статистична інформація не має містити персональних даних абонентів.

CSIRT-NBU раз на півроку публікує узагальнені статистичні дані щодо використання та ефективності роботи Системи.

**10. Інше.**

Провайдери не несуть відповідальності за точність інформації списку блокувань, отриманого від CSIRT-NBU, та діють відповідно до цього Регламенту.

Адреса технічної підтримки: вказати електронну адресу технічної підтримки CSIRT-NBU