## Порівняльна таблиця до

## РЕГЛАМЕНТУ взаємодії сторін в процесі фільтрації фішингових доменів

| РЕГЛАМЕНТ ~~роботи системи~~ фільтрації фішингових доменів<br>додаток до Розпорядження НЦУ від 30.01.2023 № 67/850 | РЕГЛАМЕНТ **взаємодії сторін в процесі** фільтрації фішингових доменів<br>Пропозиції ІнАУ |
|---|---|
| **1. Загальні положення**<br>Цей Регламент описує основні принципи та процедури взаємодії з системою фільтрації фішингових доменів (далі – Система).<br><br>Метою ~~створення Системи є фільтрація фішингових доменів у мережах операторів електронних комунікацій на рівні рекурсивних DNS серверів із використанням технології RPZ зон з метою протидії шахрайству в банківській і фінансовій сфері, пов'язаному із використанням фішингових інтернет ресурсів.~~<br><br>~~Система є складовою Національного сервісу доменних імен (DNS), створення якого передбачено пунктом 54 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», введеним в дію Указом Президента України від 1 лютого 2022 року №37.~~<br><br>Система 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". | **1. Загальні положення**<br>Цей Регламент описує основні принципи та процедури взаємодії **учасників Системи** фільтрації фішингових доменів.<br><br>Метою **співробітництва сторін є захист від фішингу банків та їх користувачів, які одночасно є абонентами операторів електронних комунікацій**.<br><br>**Виключити**<br><br>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**<br>У цьому документі наведені нижче терміни вживаються в такому значенні:<br><br>**Відсутня**<br><br>**Відсутня** | **2. Терміни та визначення**<br>У цьому документі наведені нижче терміни вживаються в такому значенні:<br><br>**фішинг (***в рамках предметної сфери Угоди)* **- незаконне заволодіння реквізитами платіжних інструментів інтернет-користувачів та інформацією, необхідною для входу до банківських систем дистанційного обслуговування**<br><br>**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)** |
| ~~провайдер~~ DNS - постачальник електронних комунікаційних мереж та/або послуг, який надає кінцевому користувачу (пов'язану) послугу з отримання інформації про домени (DNS); | **надавач сервісу** DNS **(далі - Провайдер)** - постачальник електронних комунікаційних мереж та/або послуг, який надає кінцевому користувачу (пов'язану) послугу з отримання інформації про домени (DNS); |
| учасники Системи - ~~уповноважені державні органи, провайдери DNS та інші суб'єкти господарювання, які мають санкціонований доступ до інформації в Системі з метою захисту власних електронних комунікаційних мереж~~; | учасники Системи - **CSIRT-NBU та Провайдери;** |
| **Відсутня** | **система фільтрації фішингових доменів (далі – Система) – механізм взаємодії команди реагування на кіберінциденти в банківській системі України CSIRT-NBU і провідних операторів електронних комунікацій для протидії фішингу** |
| лендінгова сторінка - інтернет-сторінка, на яку здійснюється перенаправлення запитів кінцевого користувача ~~в ході обробки DNS сервером провайдера DNS зони RPZ, яка містить перелік~~ фішингових доменів~~, які фільтруються Системою~~, та яка містить інформацію про причини такого перенаправлення; | 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; |
| ~~уповноважені державні органи - основні суб'єкти національної системи кібербезпеки, визначені Законом України "Про основні засади забезпечення кібербезпеки", підрозділ Апарату Ради національної безпеки і оборони України, який відповідає за забезпечення діяльності Національного координаційного центру кібербезпеки;~~ | **Виключити** |
| домен - символьне позначення областей в мережі Інтернет, що базується на ієрархічній структурі, що дозволяє визначити доменні імена; | **Виключити, оскільки визначення міститься в законодавстві України** |
| доменне ім'я - символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі; | **Виключити, оскільки визначення міститься в законодавстві України** |
| IP адреса - мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP; | **Виключити, оскільки визначення міститься в законодавстві України** |

| | |
|---|---|
| DNS - комп'ютерна розподілена система для отримання інформації про домени;<br><br>RPZ. (Response Policy Zones) - стандартизований механізм застосування політик обробки запитів на серверах DNS. RPZ зона - зона DNS, в якій застосовується відповідна політика фільтрації доменів.<br><br>**Відсутня**<br><br>Інші терміни у цьому документі вживаються у значеннях, визначених законодавством України. | DNS - комп'ютерна розподілена система для отримання інформації про домени;<br><br>**Виключити**<br><br>**API – набір визначених методів для запиту даних, аналізу, обробки та надсилання відповіді на запити.**<br><br>Інші терміни у цьому документі вживаються у значеннях, визначених законодавством України. |
| **3. Принципи фільтрації доменів**<br>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.<br>*Основні засади функціонування Системи:*<br>1. Використання стандартизованого механізму для фільтрації фішингових доменів, ~~а саме методу DNS RPZ.~~<br>2. Фільтрація фішингового домену відбувається у період з моменту його виявлення до видалення (призупинення дії) домену на рівні реєстратора доменних імен.<br>3. Фільтрація відбувається на рівні рекурсивних DNS серверів українських постачальників електронних комунікаційних ~~мереж та/або~~ послуг.<br>4. З метою підвищення обізнаності користувачів інтернет ~~реалізовано~~ безпечну лендінгову сторінку, на яку здійснюється перенаправлення запитів до фішингових ресурсів. Ця сторінка забезпечує інформування користувачів про потенційний ризик, а також механізм зворотного зв'язку. | **3. Принципи фільтрації доменів**<br>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.<br>*Основні засади функціонування Системи:*<br>1. Використання стандартизованого механізму **API** для **отримування списку** фішингових доменів **для подальшого контролю та включення до блокування.**<br>2. **Процес** фільтрації **Провайдером** фішингового домену відбувається у період з моменту його виявлення до видалення (призупинення дії) домену на рівні реєстратора доменних імен.<br>3. Фільтрація відбувається на рівні рекурсивних DNS серверів українських постачальників електронних комунікаційних послуг.<br>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. | 5. Для обліку доменів та централізованого зберігання використовується окрема подія платформи MISP, для систематизації переліку фішингових доменів використовується необхідний набір тегів. |
| 6. ~~Для забезпечення максимальної ефективності Системи необхідно мінімізувати час з моменту виявлення шкідливого домену до моменту фільтрації. Частота оновлення RPZ зони - до 15 хвилин з моменту внесення змін до переліку фішингових доменів.~~ | **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. ~~Синхронізація RPZ зони відбувається від авторитетного серверу до рекурсивних серверів провайдерів DNS з використанням стандартизованих механізмів AXFR (повна передача зони DNS RFC5936) та IXFR (інкрементальна передача зони DNS RFC1995).~~ | **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.** *(Коментар: Оскільки механізм RPZ не дає можливості для необхідної модерації на стороні провайдера, пропонується по API. MISP API буде приймати і оброблювати запити від клієнтів (провайдерів) з використанням токена. Використання двох методів (full та increment) дозволить раціонально використовувати ресурси та передавати тільки необхідні зміни.* |
| *Основні компоненти Системи:* | *Основні компоненти Системи:* |
| 1. Платформа MISP (адреса публікації ~~https://fmisp.ncscc.gov.ua~~) | 1. Платформа MISP (адреса публікації **https://misp.bank.gov.ua/**) |
| Платформа MISP забезпечує доступ учасників Системи до актуального переліку фішингових доменів. Перелік фішингових доменів ~~реплікується в автоматичному режимі із MISP-NBU.~~ Учасники Системи можуть використовувати платформу MISP для надання пропозиції до переліку фішингових доменів. | 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 пропозиції до переліку фішингових доменів. |
| | **Будь-які транзитні сервери не можуть використовуватись у системі задля уникнення можливості компрометації інформації.** |
| ~~2. Авторитетний сервер DNS (IP адреса публікації 185.13.250.11)~~ | **Виключити** |
| ~~Авторитетний сервер DNS здійснює обслуговування RPZ зони "fraud-roz.ua.db", яка автоматизовано оновлюється у відповідності до переліку фішингових доменів у платформі MISP, та виступає провайдером для реплікації RPZ зони для рекурсивних DNS серверів учасників Системи.~~ | |
| 3. Лендінгова сторінка (~~IP адреса публікації 185.13.250.10~~) | 2. Лендінгова сторінка |

| | |
|---|---|
| Інтернет-сторінка, на яку здійснюється перенаправлення кінцевого користувача до фішингового домену.<br><br>~~4.Рекурсивні DNS сервери учасників Системи~~<br>~~Рекурсивні сервери учасників Системи, що здійснюють обслуговування клієнтських запитів із застосуванням політик RPZ.~~<br>~~За потреби учасники Системи можуть використовувати проміжні DNS сервери для централізованого розповсюдження RPZ зони у середині своєї мережі.~~<br>~~За погодженням з власником Системи допускається, щоб провайдери DNS синхронізували RPZ зону від інших провайдерів DNS, наприклад, по регіональному чи ієрархічному принципу~~ | Інтернет-сторінка **Провайдера**, на яку здійснюється перенаправлення **запитів** кінцевого користувача **на домени з переліку фішингових доменів**. **Вимоги до лендінгової сторінки встановлені у розділі 8.**<br><br>**Виключити** |
| **4. Організація взаємодії з Системою**<br>Для отримання доступу до Системи провайдер DNS здійснює реєстрацію в Системі шляхом надсилання заявки на адресу ~~fraud-filter@ncscc.gov.ua~~.<br><br>Заявка провайдера DNS на реєстрацію в Системі повинна містити: назву провайдера DNS та код ЄДПРОУ/ІПН, ПІБ та адресу електронної пошти уповноваженої особи, IP адресу(-и) власного DNS серверу, ~~який здійснює синхронізацію зони RPZ. Додатково провайдер DNS може вказати перелік власних підмереж (AS) для доступу до статистичних даних щодо роботи Системи, назву і версію програмного забезпечення власного DNS серверу для отримання технічних рекомендацій з його налаштування.~~<br><br>Відповідно до наданих провайдером DNS в заявці на реєстрацію даних в платформі MISP за адресою https://fmisp.ncscc.gov.ua створюється користувач з правами "org admin", який має права створювати додаткових користувачів з представників своєї організації.<br>Учасники Системи відповідають за підтримку реєстраційних даних в актуальному стані.<br>Після реєстрації, провайдер DNS налаштовує на власному DNS сервері ~~синхронізацію зони RPZ «fraud-rpz.ua.db».~~ | **4. Організація взаємодії з Системою**<br>Для отримання доступу до Системи Провайдер здійснює реєстрацію в Системі шляхом надсилання заявки на **електронну адресу MISP-NBU** вказати електронну адресу MISP-NBU<br><br>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**.<br><br>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.<br>Учасники Системи відповідають за підтримку реєстраційних даних в актуальному стані.<br>Після реєстрації Провайдер налаштовує на власному DNS сервері **взаємодію для отримання списку блокувань.** |

| | |
|---|---|
| ~~Реєстрація в Системі уповноважених державних органів здійснюється на підставі листа-запиту до Апарату Ради національної безпеки і оборони України, що містить ПІБ та адресу електронної пошти уповноваженої особи.~~ | **Виключити** |
| **5. Внесення доменів до зони RPZ**<br>~~Відповідальність за~~ ведення переліку фішингових доменів покладається на галузеву команду реагування на кіберінциденти у банківській системі України Національного банку України CSIRT-NBU (далі - CSIRT-NBU). Для зберігання та розповсюдження переліку фішингових доменів використовується платформа MISP.<br>Команда CSIRT-NBU розглядає звернення від основних суб'єктів забезпечення кібербезпеки України та учасників Системи щодо внесення доменів до переліку фільтрації. Команда CSIRT-NBU проводить періодичний перегляд статусів доменів із метою мінімізації переліку. Фільтрації підлягають тільки активні домени, не заблоковані реєстраторами доменних імен.<br><br>**Відсутня**<br><br>**Відсутня**<br><br>Пропозиції учасників Системи щодо внесення доменів до ~~зони RPZ надаються на адресу~~ fraud-filter@ncscc.gov.ua ~~та/або через механізм "proposals" в екземплярі MISP за адресою~~ https://fmisp.ncscc.gov.ua~~.~~<br><br>Пропозиції щодо внесення доменів ~~до зони RPZ~~ розглядаються протягом робочого часу. Строк обробки пропозиції ~~щодо внесення домену до зони RPZ~~ - дві години з часу надання пропозиції.<br><br>Користувачі інтернет, які виявили фішинговий домен, мають право надати пропозиції щодо внесення доменів до зони RPZ через учасників Системи та/або Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA. | **5. Внесення доменів до списку блокувань.**<br>Ведення переліку фішингових доменів покладається на галузеву команду реагування на CSIRT-NBU. Для зберігання та розповсюдження переліку фішингових доменів використовується платформа MISP-**NBU**.<br><br>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.<br><br>**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.**<br><br>**Перелік фішингових доменів затверджується за допомогою кваліфікованого електронного підпису керівника Команди CSIRT-NBU чи іншої уповноваженої ним особи.**<br><br>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**.**<br><br>Пропозиції щодо внесення доменів **до списку блокувань** розглядаються протягом робочого часу. Строк обробки пропозиції дві години з часу надання пропозиції.<br><br>**Виключити** |
| **6. Вилучення доменів із ~~зони RPZ~~** | **6. Вилучення доменів із списку блокувань.** |

| | |
|---|---|
| Пропозиції щодо вилучення доменів із ~~зони RPZ~~ можуть надаватися усіма учасниками Системи. Остаточне рішення про вилучення доменів ~~із зони RPZ~~ приймає CSIRT-NBU.<br><br>Пропозиції учасників Системи щодо вилучення доменів ~~із зони RPZ~~ надаються на ~~адресу~~ fraud-filter@ncscc.gov.ua ~~та/або через механізм "proposals" в екземплярі MISP за адресою~~ https://fmisp.ncscc.gov.ua~~.~~<br><br>Власник або адміністратор домену, який вважає, що його домен помилково внесено до ~~зони RPZ,~~ надсилає мотивовану заявку на виключення домену на електронну адресу, вказану на лендінговій сторінці. Заявка повинна містити ідентифікацію особи та підтвердження права власності на домен.<br><br>Пропозиції щодо вилучення домену із зони RPZ розглядаються під час робочого часу. Строк оновлення RPZ зони складає до 15 хвилин з моменту внесення змін до переліку доменів. | 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.<br>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**.**<br><br>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.<br>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**<br>З метою зменшення ризику помилкового внесення не фішингових доменів до зони RP/ Система використовує механізм білих списків доменів. До білого списку внесені домени, які заборонено фільтрувати за допомогою Системи.<br>Пропозиції щодо додавання доменів до білого списку можуть надаватися усіма учасниками Системи . Остаточне рішення про внесення доменів до білого списку приймає CSIRT-NBU.<br>Користувачі інтернет мають право надати пропозиції щодо внесення доменів до білого списку через учасників Системи. | **7. Білі списки доменів**<br>**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**<br>Лендінгова сторінка повинна містити:<br>• попередження користувачу інтернет про небезпеку переходу на фішинговий ресурс;<br>• доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід<br>• поточну дату та час<br>• адресу електронної пошти для подання заявки на виключення домену із зони RPZ.<br>Додатково лендінгова сторінка може містити рекомендації з кібербезпеки для користувачів інтернет. | **8. Вимоги до лендінгової сторінки Провайдера.**<br>Лендінгова сторінка повинна містити:<br>• попередження користувачу інтернет про небезпеку переходу на фішинговий ресурс;<br>• доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід<br>• поточну дату та час<br>• адресу електронної пошти для подання заявки на виключення домену із **списку блокувань**.<br>Додатково лендінгова сторінка може містити рекомендації з кібербезпеки для користувачів інтернет. |

| | |
|---|---|
| **9. Статистика та звітність**<br>При переході на лендінгову сторінку у Системі зберігається технічна інформація, що включає дату і час, ~~IP-адресу (підмережу), з якої здійснюється перехід,~~ доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід~~, user-agent тощо~~.<br><br>~~Система має інтерфейс для доступу до інформації щодо переходів на лендінгову сторінку~~.<br>Провайдерам DNS за запитом надається інформація щодо переходів на лендінгову сторінку з їх підмереж за умови надання списку їх підмереж (AS) під час реєстрації.<br><br>~~З метою аналізу та відповідного реагування уповноваженим державним органам надається доступ до інформації щодо переходів на лендінгову сторінку.~~<br>CSIRT-NBU раз на півроку публікує ~~та надає до НКЦК~~ узагальнені статистичні дані щодо використання та ефективності роботи Системи. | **9. Статистика та звітність**<br>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.<br><br>**Виключити**<br><br>**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.**<br><br>**Виключити**<br><br>CSIRT-NBU раз на півроку публікує узагальнені статистичні дані щодо використання та ефективності роботи Системи. |
| **10. Інше**<br>Провайдери DNS не несуть відповідальності за точність інформації в зоні RPZ, фільтрацію доменів у відповідності до цього Регламенту.<br><br>~~Власником Системи є Національний координаційний центр кібербезпеки в особі структурного підрозділу Апарату Ради національної безпеки і оборони України, який відповідає за забезпечення діяльності НКЦК.~~<br>~~Текст цього Регламенту публікується за адресою https://fmisp.ncscc.gov.ua/reglament. В разі внесення змін до цього Регламенту власник Системи повідомляє учасників Системи не менше ніж за 10 робочих днів до набрання чинності таких змін шляхом направлення повідомлень на електронну пошту учасників, зазначених ними під час реєстрації в Системі.~~<br>Адреса технічної підтримки: fraud-filter@ncscc.gov.ua. | **10. Інше**<br>Провайдери не несуть відповідальності за точність інформації списку блокувань, отриманого від CSIRT-NBU, та діють відповідно до цього Регламенту.<br>**Виключити**<br><br>**Виключити**<br><br>Адреса технічної підтримки:_____ |