# Чи можна використовувати електронну пошту як фактор багатофакторної автентифікації

IT · https://nasu.com.ua/mdata/chy-mozhna-vykorystovuvaty-elektronnu-poshtu-yak-faktor-bagatofaktornoyi-avtentyfikacziyi/

Чи може страховик використовувати надсилання коду або повідомлення на електронну адресу користувача як один із факторів багатофакторної автентифікації за пунктом 20 Постанови № 143, а не лише на номер телефону (SMS, Viber тощо)?

У пункті 20 розділу II Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг, затвердженого постановою Правління Національного банку України від 09.12.2025 № 143 (далі – Положення № 143), встановлено обов’язок надавача фінансових послуг запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів під час здійснення ними віддаленого доступу до інформаційно-комунікаційних систем.

Водночас наведена норма не визначає конкретної технології або каналу реалізації багатофакторної автентифікації (далі – MFA), що відповідає принципу технологічної нейтральності регулювання, та відповідно, не забороняє використання електронної пошти як одного з каналів MFA.

Разом з тим застосування будь-якого механізму MFA має відповідати основній меті багатофакторної автентифікації – забезпеченню використання незалежних факторів автентифікації, компрометація одного з яких не повинна автоматично призводити до компрометації інших факторів.

Використання електронної пошти як каналу доставки одноразових кодів автентифікації (OTP), хоча і може, формально, забезпечувати використання другого кроку автентифікації, однак має суттєві обмеження.

З урахуванням сучасної практики кіберзахисту найдоцільнішим є:

– застосовування механізмів MFA, що забезпечують незалежність факторів автентифікації;

– не використовувати електронну пошту як основний канал MFA для віддаленого доступу користувачів та привілейованих користувачів;

– пріоритет використання криптографічно захищених механізмів автентифікації (наприклад: FIDO2/WebAuthn, апаратних токенів, TOTP-додатків або інших еквівалентних рішень);

– використання електронної пошти як резервного механізму відновлення доступу або як тимчасового фактора ідентифікації до впровадження більш захищених способів MFA.

Лист НБУ № 33-0007/74391 від 08.08.2026