Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
Частина 4 розділу I Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг 4. Вимоги цього Положення не поширюються на надавачів платіжних та супровідних послуг, а також операторів поштового зв'язку, що мають право здійснювати діяльність з торгівлі валютними цінностями.	Пропонується запропоновану частину 4 викласти в такій редакції: 4. Вимоги цього Положення не поширюються на надавачів платіжних та супровідних послуг, а також операторів поштового зв'язку, що мають право здійснювати діяльність з торгівлі валютними цінностями **в частині що не стосується діяльності з надання фінансових послуг**.	Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг розроблено відповідно до вимог Законів України "Про НБУ" та "Про фінансові послуги та фінансові компанії" які визначають наявність повноважень НБУ для встановлення для надавачів фінансових послуг вимог інформаційної безпеки та кіберзахисту на ринках фінансових послуг. Зважаючи на те, що НБУ не оприлюднив для обговорення положення щодо забезпечення вимог інформаційної безпеки та кіберзахисту на ринках фінансових послуг для надавачів платіжних та супровідних послуг, та операторів поштового звязку, особливо зважаючи на дію воєнного стану - необхідним є забезпечення такими субєктами належної інформаційної безпеки та кіберзахисту. НБУ не оприлюднив підтверджень що вказують що за результатами оцінювання такі субєкти вже мають достатній рівень інформаційної безпеки та кіберзахисту. Таким чином є недопустими та не послідовним дії НБУ щодо незабезпечення дотримання відповідних вимог інформаційної безпеи та кіберзахисту надавачами платіжних та супровідних послуг, а також операторів поштового звязку. В звязку з чим мною як користувачем даних послуг таких субєктів з метою отримання фінансових послуг що надаються вказаними субєктами вважається сумнівним та недоцільним виключення цих категорій із вказаних вимог. Таким чином я обгрунтовую доцільність поширення цих вимог і на вказані категорії надавачів фіансових послуг.	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Абзаци 2 та 3 частини 23 Розділу I Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	Виключити абзаци 2 та 3 частини 23 Розділу I	НБУ надає прямі вимоги до технологій які мають бути використані чи не використані. При цьому відсутнє належне обгрунтування доведеності чому такі технології є недостатніми, а інші технології мають бути застосовані в обовязковому порядку. Таким чином такі вимоги суперечать іншім вимогам в частині побудови ризик-орієнтованої системи та загального права субєкта господарювання на право діяльності та вільного вибору технологій забезпечення захисту які не є вцілому заборонені. Пготенційно така заборона може мати місце для категорій інформацій яка є відповідного рівня доступу - але не вцілому для всієї системи що є анадто обтяжливою та недоречною.	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32

Частина 24 Розділу I 24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування); 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів; 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем; 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	Пропонується викласти в такій редакції: 24. Надавач фінансових послуг зобов'язаний забезпечити блокування/**видалення** облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) **декількох (до п'яти)** невдалих спроб автентифікації поспіль (автоматичне блокування) - **блокування на строк до 1 години**; 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів **- блокування на строк до авторизації особи користувача в безпечний доведений спосіб та передачі його оновлених способів та методів авторизації**; 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем - **видалення такого облікового запису разом із забезпечення збереження архівувної копії всіх даних повязаних із його діяльністю**; 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок **в частині послуг які передбачають обовязковість членства у кредитній спілці) - видалення такого облікового запису разом із забезпечення збереження архівувної копії всіх**	Уточнення в частині що можуть бути випадки коли необхідно і видалити обліковий запис чи поновити доступ.	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Частина 28 Розділу I 28. Надавач фінансових послуг зобов'язаний забезпечити маскування значення паролю при введенні його клієнтом, користувачем та привілейованим користувачем.	Виключити дане положення	Для систем побудованих на доступі через браузер дана можливість (маскування) реалізовано на рівні браузеру тому така вимога виключить можливість застосування такого виду доступу для практично всіх надавачів фінансових послуг та онлайн банкінг	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Частина 30 Розділу I 30. Надавач фінансових послуг зобов'язаний забезпечити автоматичне блокування робочого столу операційної системи на робочій станції або сервері, якщо немає активності користувача протягом 15 хвилин, з наступною повторною автентифікацією користувача під час розблокування (за винятком робочих станцій або серверів, на яких блокування неможливе або потребує більшого інтервалу часу відсутності активності за технологією використання).	Додати частинку "до" перед виразом 15 хвилин Частина 30 Розділу I 30. Надавач фінансових послуг зобов'язаний забезпечити автоматичне блокування робочого столу операційної системи на робочій станції або сервері, якщо немає активності користувача протягом **до** 15 хвилин, з наступною повторною автентифікацією користувача під час розблокування (за винятком робочих станцій або серверів, на яких блокування неможливе або потребує більшого інтервалу часу відсутності активності за технологією використання).	Нормування саме 15 хвилин є зайвим для систем які мають значно вищі вимоги - тому достатнім є граничне обмеження строку в до 15 хвилин	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Частина 31 Розділу I 31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	Виключити вираз "(за ідентифікатором управління доступом до обладнання, MAC-адресою)"	Відстунє нормативне термінологічне визначення даних визначень "ідентифікатор управління доступу до обладнання" (відсутнє в жодних вказанх стандартах на які посилається розробник даного акту)	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Частина 32 Розділу I 32. Надавач фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг в спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події:	Доповнити новим підпунктом 9 9) реєстрація подій щодо оновлення будь-яких контактних та інших даній які є дозволеними клієнтам, користувачам та привілейованим користувачам	Уточнення щодо необхідності ведення логів подій щодо оновлення/зміни даних які дозволені до редагування користувачу. Наприклад контаткний номер телефону…	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32
Частина 46 Розділу I 46. Надавач фінансових послуг зобов'язаний забезпечити розміщення в демілітаризованій зоні інформаційно-комунікаційних систем надавача фінансових послуг, серверів та обладнання, що забезпечує функціонування сервісів (надання послуг), які відкриті для доступу клієнтів з зовнішніх мереж.	Виключити дане положення	Неможливо розмістити в демілітирозваній зоні таке обладнання так як демілітиризована зона це підмережа яка відокремлює внутрішню мережу від електронної комунікаційної мережі загального користування та мережі Інтернет. А таке обладнання/сервери забезпечують функціонування серсівіс і вони перебувають не в демілітиризованій зоні в тому значенні як запропоновано - а в внутрішній мережі	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32

Частина 48 Розділу I 48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість:	Виключити термін "для яких не припинено підтримку виробника та"	Так як наприклад більшість банкоматів працюють під управлінням Windows XP яка вже не підтримується, що призведе до необгрунтованої зміни обладнання так як виробник кінцевого обладнання забезпечує безпечність роботи таких систем навіть з використанням такої не "актуальною" операційною системою. Так само і відкриті системи на базі Linux - це є відкритий код і відсутнє значення хто є "виробник"	Фізична особа: Кушніренко Павло Борисович	pavlo.kushnirenko@gmail.com	12.03.2025 04:32:32

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
12. Керівник надавача фінансових послуг: ... 2) призначає відповідальну особу за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг та здійснює контроль за їхньою діяльністю;	12. Керівник надавача фінансових послуг: ... 2) **може** призначити **відповідальну** особу за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг та здійснює контроль за їхньою діяльністю, **або виконувати ці функції самостійно**;	Призначення окремої особи на цю позицію створить значне фінансове навантаження на малий бізнес. У малих компаніях функції з інформаційної безпеки та кіберзахисту можуть ефективно виконуватися керівником, з огляду на обмежену кількість персоналу та менший обсяг інформаційних систем.			
14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: … 3) ~~організовує~~ регулярну, але не рідше одного разу на рік ~~з моменту останньої проведеної інвентаризації, інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг~~; … 6) уживає заходів щодо недопущення встановлення та використання в складі інформаційно-комунікаційних систем програмних і апаратних засобів, ~~що не передбачені внутрішніми документами надавача фінансових послуг~~;	14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: … 3) **формує та проводить** регулярну, але не рідше одного разу на рік, **актуалізацію реєстру інформаційних активів надавача фінансових послуг, включаючи власників цих активів**; … 6) уживає заходів щодо недопущення встановлення **та використання** в складі інформаційно-комунікаційних систем програмних і апаратних засобів **надавача фінансових послуг без тестування і узгодження вимог інформаційної безпеки і кіберзахисту**;	Управління програмними, апаратними засобами та їх конфігураціями (CMS/CMDB) відповідно до мжнародного стандарту ITIL функція напрямку IT. Функція ІБ, відповідно до контролю 5.9 ДСТУ ISO 27001 це розробка та підтримка інвентаризації інформації та інших пов'язаних активів, включаючи власників. Якщо все ж таки мова тут про CMS/CMDB, то функція відповідальної особи за ІБ та КБ це контроль за управлінням, тоді пропонуємо наступну редакцію: 14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 3) проводить регулярний, але не рідше одного разу на рік з моменту останнього проведеного контролю, контроль обліку програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг та за результатами проведення контролю формує звіт керівництву фінансової установи;	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 5) організовує контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг та забезпечують відновлення їх працездатності в разі порушення штатного режиму функціонування;	4. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 5) організовує контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг **за результатами якого надає рекомендації технічним підрозділам щодо** відновлення їх працездатності в разі порушення штатного режиму функціонування;	Відновлення працездатності засобів захисту інформації в інформаційно-комунікаційних системах в разі порушення штатного режиму функціонування, це пряма функція технічного підрозділу IT напрямку.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
17. Надавач фінансових послуг зобов'язаний забезпечити розподіл прав доступу до інформаційно-комунікаційних систем в спосіб, що дозволятиме: … 2) здійснити опис груп, ролей та розподіл повноважень клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем (~~шаблонно-рольова модель~~);	17. Надавач фінансових послуг зобов'язаний забезпечити розподіл прав доступу до інформаційно-комунікаційних систем в спосіб, що дозволятиме: … 2) здійснити опис груп, ролей та розподіл повноважень клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем (**шаблони моделей доступу**);	Сучасні інформаційні системи використовують окрім рольових моделей доступу (RBAC) вже і атрибутні моделі доступу (ABAC) і досі існують і інші моделі доступу: DAC і MAC. Тому пропонується більш загальна фраза.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
22. Надавач фінансових послуг зобов'язаний організувати та забезпечити доступ клієнтів, користувачів та привілейованих користувачів інформаційно комунікаційних систем надавача фінансових послуг в межах встановлених для них прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) клієнта, користувача, привілейованого користувача і паролю, що вводиться клієнтом, користувачем, привілейованим користувачем, або програмно-апаратного ідентифікатора (ключ, сертифікат, токен).	22. Надавач фінансових послуг зобов'язаний організувати та забезпечити доступ клієнтів, користувачів та привілейованих користувачів інформаційно комунікаційних систем надавача фінансових послуг в межах встановлених для них прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) клієнта, користувача, привілейованого користувача і паролю, що вводиться клієнтом, користувачем, привілейованим користувачем, або програмно-апаратного ідентифікатора (ключ, сертифікат, токен, **біометрія**).	Біометрія – це така саме комплексна технологією, яка поєднує як апаратні засоби, так і програмне забезпечення, для проведення ідентифікації і автентифікації, як і ключ, сертифікат, токен.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
26. Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менш ніж ~~12~~ символів та містять цифри, букви в різних регістрах та спеціальні символи.	26. Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менш ніж **15** символів та містять цифри, букви в різних регістрах та спеціальні символи.	В останніх рекомендаціях best practices довжина паролю пропонується не менше 15 символів. В цьому випадку мова йде про привілейованих користувачів і це підвищені ризики, тому не можна пом'якшувати відомі світові вимоги з інформаційної безпеки і кіберзахисту.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54

27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на ~~60~~ днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі в разі компрометації, але не рідше одного разу на **90** днів **або в разі виявлення в базах скомпрометованих паролів**. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	В настановах best practices оновлених у 2024 року пропонується не змушувати користувачів періодично змінювати паролі, а приділяти більшу увагу унікальності і довжині паролів. Зараз більшість використовує період зміни паролю 90 днів. Скорочення періоду не призведе до пом'якшення ризиків, але може викликати роздратування користувачів.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
29. Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування облікових записів привілейованих користувачів інформаційно-комунікаційних систем, що встановлюються за замовчуванням (за наявності технічної можливості та за умови збереження функціонування інформаційно-комунікаційних систем), та відключення гостьових облікових записів.	29. Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування облікових записів привілейованих користувачів інформаційно-комунікаційних систем **та облікових записів користувачів операційних систем,** що встановлюються за замовчуванням (за наявності технічної можливості та за умови збереження функціонування інформаційно-комунікаційних систем), та відключення гостьових облікових записів.	Вимоги викладені у наведених пунктах ідентичні. Пропозиція доповнити п.29 (виділено напівжирним), а п.49. вилучити.			
49. Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів.	~~49. Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів.~~				
31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, ~~MAC-адресою~~), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за апаратним ідентифікатором управління доступом до обладнання, **сертифікатами, за допомогою спеціалізованого програмного забезпечення**), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	Не можна звужувати ідентифікатор управління доступом до обладнання виключно до MAC-адреси. Тому, що за апаратними характеристиками існують ще UUID (Унікальний ідентифікатор пристрою), IMEI та серійний номер, тощо. А окрім апаратних характеристик можна управляти доступом за допомогою сертифікатів або за допомогою спеціального програмного забезпечення, яке збирає та передає унікальну інформацію про пристрій для подальшої ідентифікації при підключенні до сервера.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
32. фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг в спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події: … 3) реєстрація подій, пов'язаних із управлінням правами доступу до інформаційно-комунікаційних систем та інформації, що циркулює в них; … 6) реєстрація, видалення (блокування) облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах;	32. фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг в спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події: … 3) реєстрація подій, пов'язаних із управлінням правами доступу **користувачів та привілейованих користувачів** до інформаційно-комунікаційних систем та інформації, що циркулює в них; … 6) реєстрація, видалення (блокування) облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах;	«реєстрація, видалення (блокування) облікових записів клієнтів» - це і є події, які пов'язані із управлінням правами доступу. Реєстрація та видалення облікових записів є невід'ємними частинами управління правами доступу, оскільки через облікові записи визначають, хто має доступ та які саме права їм надаються.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54
34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити ~~їх~~ зберігання не менше одного року з моменту архівації, якщо інше не передбачено законодавством.	34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити зберігання **журналів реєстрації подій** не менше одного року з моменту архівації, якщо інше не передбачено законодавством.	Замінено займенник "їх", який може створювати неясність щодо того, що саме повинно зберігатися, зміна допомагає уточнити, що саме має бути збережене — саме "журнали реєстрації подій". Цей зміст має більше чіткості, а ця зміна сприяє підвищенню зрозумілості та точності тексту.	Юридична особа: ТОВ "НоваПей Кредит"	ЄДРПОУ: 40055034, (office@novapay.ua)	21.03.2025 09:39:54

51. Надавач фінансових послуг зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і мають містити положення щодо: … 3) ідентифікації змінних носіїв інформації, які використовуються надавачем фінансових послуг;	51. Надавач фінансових послуг зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і мають містити положення щодо: … 3) **обов'язкової** ідентифікації змінних носіїв інформації, які використовуються надавачем фінансових послуг **за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія**;	Поєднання вимог з обов'язкової ідентифікації змінних носіїв інформації в один пункт.
52. Надавач фінансових послуг зобов'язаний здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія.	~~52. Надавач фінансових послуг зобов'язаний здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія.~~	

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
2. Надавачам фінансових послуг протягом шести місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	2. Надавачам фінансових послуг протягом **двадцяти чотирьох** ~~шести~~ місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	Для впровадження всіх вимог, які передбачені Положенням потрібно здійснити закупівлю обладнання, в тому числі достатньо дороговартісного, зміни у процесах, програмному забезпеченні, що буде вимагати додаткових витрат на розробників програмного забезпечення, та провести навчання персоналу. В умовах війни такі витрати будуть не співмірними з можливими збитками від подій кіберінцеденту, особливо для невеликих кредитних спілок з їх обмеженим ресурсом. При цьому, у міжнародній практиці для подібних змін надають принаймні від 12 до 24 місяців, що дає змогу зменшити фінансове навантаження на кредитну спілку.			
Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
I. Загальні положення	I. Загальні положення	I. Загальні положення	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
2. Терміни в цьому Положенні вживаються в таких значеннях: 2) демілітаризована зона – фізична або логічна підмережа яка відокремлює внутрішню мережу [інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи (далі – інформаційно-комунікаційна система)] надавача фінансових послуг від електронної комунікаційної мережі загального користування та мережі Інтернет; 4) кіберризик – ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз; є складовою операційного ризику;	2. Терміни в цьому Положенні вживаються в таких значеннях: 2) **зона мережі з підвищеним рівнем безпеки** ~~демілітаризована~~ ~~зона~~ – фізична або логічна підмережа яка відокремлює внутрішню мережу [інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи (далі – інформаційно-комунікаційна система)] надавача фінансових послуг від електронної комунікаційної мережі загального користування та мережі Інтернет; 4) кіберризик – ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз. **Кіберризик є ризиком інформаційної безпеки**; ~~є складовою операційного ризику~~;	до пп. 2) у проєкті положення використовується термін "демілітаризована зона" для опису підмережі, що відокремлює внутрішню мережу надавача фінансових послуг від мережі Інтернет. Цей термін не є стандартним у ДСТУ ISO/IEC 27001:2023 та ДСТУ ISO/IEC 27002:2023, де використовується поняття "зони мережі з підвищеним рівнем безпеки" (secure network zones). до пп. 4) відповідно до пп. 40 п. 2 Положення НБУ № 15 кіберризик є складовою саме ризику інформаційної безпеки		
7) основні бізнес-процеси – дії, операції, завдання, що виконуються структурними підрозділами, окремими працівниками надавача фінансових послуг, інформаційними системами (включаючи функції, передані на аутсорсинг), що мають безпосередній та істотний вплив на досягнення цілей діяльності надавача фінансових послуг, та порушення здійснення контрольних заходів щодо таких дій, операцій, завдань може завдати істотних збитків надавачу фінансових послуг або його користувачам та/або може призвести до порушення вимог законодавства України;	7) основні бізнес-процеси – сукупність взаємопов'язаних або взаємодіючих видів діяльності, спрямованих на створення певного продукту або послуги дії, операції, завдання, що виконуються структурними підрозділами, окремими працівниками надавача фінансових послуг, інформаційними системами (включаючи функції, передані на аутсорсинг), що мають безпосередній та істотний вплив на досягнення цілей діяльності надавача фінансових послуг, та порушення здійснення контрольних заходів щодо таких дій, операцій, завдань може завдати істотних збитків надавачу фінансових послуг або його користувачам та/або може призвести до порушення вимог законодавства України;	до пп. 7) як в теорії та міжнародній практиці, так й в нормативно-правових актах НБУ, зокрема пп. 2 п. 2 Положення НБУ № 15, основні бізнес-процеси це ті дії, які направлені саме на створення продукту та послуги. В той же час, наведене в проєкті Положення формулювання відповідає визначенню "процесу", а не "основному бізнес-процесу".	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

5. Надавач фінансових послуг зобов'язаний вживати заходів із забезпечення інформаційної безпеки та кіберзахисту до об'єктів захисту, що встановлені цим Положенням, якими є: *** 3) інформаційно-комунікаційні системи надавача фінансових послуг, що підтримують ключові та/або критичні бізнес-процеси надавача фінансових послуг та/або взаємодіють з інформаційними системами Національного банку.	5. Надавач фінансових послуг зобов'язаний вживати заходів із забезпечення інформаційної безпеки та кіберзахисту до об'єктів захисту, що встановлені цим Положенням, якими є: *** 3) інформаційно-комунікаційні системи надавача фінансових послуг, що підтримують **основні** ~~ключові~~ ~~та/або~~ ~~критичні~~ бізнес-процеси надавача фінансових послуг та/або взаємодіють з інформаційними системами Національного банку.	Проект Положення та інші нормативно-правові акти не містять визначення ключових або критичних бізнес-процесів. В той же час, відповідно до пп. 3 ч. 2 ст. 4 ЗУ Про основні засади забезпечення кібербезпеки України об'єктами кіберзахисту є комунікаційні системи, **які використовуються для задоволення суспільних потреб** та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу. Таким чином, вимоги цього положення повинні розповсюджуватися саме на ті інформаційні системи, **які використовуються для створення та підтримки продуктів та послуг фінансової установи** (тобто, задоволення суспільних потреб), що як в теорії та міжнародній практиці, так й в нормативно-правових актах НБУ, зокрема пп. 2 п. 2 Положення НБУ № 15, є основним бізнес-процесом.			
II. Базові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту	II. Базові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту	II. Базові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
12. Керівник надавача фінансових послуг: *** 3) затверджує внутрішні документи з питань забезпечення інформаційної безпеки та кіберзахисту, уключаючи політики за окремими напрямами діяльності, положення, стандарти, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі, відповідно до вимог цього Положення;	12. Керівник надавача фінансових послуг: *** 3) затверджує внутрішні документи з питань забезпечення інформаційної безпеки та кіберзахисту, уключаючи політики ~~за окремими напрямами діяльності~~, положення, стандарти, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі, відповідно до вимог цього Положення;	в даному разі інформаційна безпека та кіберзахист саме й є окремими напрямами діяльності	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 1) забезпечує виконання вимог з інформаційної безпеки та кіберзахисту, що встановлені цим Положенням; 2) розробляє політику інформаційної безпеки відповідно до вимог цього Положення; 3) організовує регулярну, але не рідше одного разу на рік з моменту останньої проведеної інвентаризації, інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг; 4) здійснює моніторинг та розслідування інцидентів інформаційної безпеки та кіберінцидентів; 5) організовує контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг та забезпечують відновлення їх працездатності в разі порушення штатного режиму функціонування; 6) уживає заходів щодо недопущення встановлення та використання в складі інформаційно-комунікаційних систем програмних і апаратних засобів, що не передбачені внутрішніми документами надавача фінансових послуг;	14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 1) забезпечує виконання вимог з інформаційної безпеки та кіберзахисту, що встановлені цим Положенням; 2) розробляє **внутрішні документи з питань** ~~політику~~ інформаційної безпеки відповідно до вимог цього Положення; ~~3) організовує регулярну, але не рідше одного разу на рік з моменту останньої проведеної інвентаризації, інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг;~~ 4) здійснює моніторинг та розслідування інцидентів інформаційної безпеки та кіберінцидентів; 5) організовує контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг та забезпечують відновлення їх працездатності в разі порушення штатного режиму функціонування; 6) уживає заходів щодо недопущення встановлення та використання в складі інформаційно-комунікаційних систем програмних і апаратних засобів, що не передбачені внутрішніми документами надавача фінансових послуг;	до пп. 2) питання інформаційної безпеки може регулюватися не тільки політикою до пп. 3) відповідно до ст. 10 ЗУ Про бухгалтерський облік та фінансову звітність в Україні та Положення про інвентаризацію активів та зобов'язань, затверджене наказом Мінфіна від 02.09.2014 № 879 інвентаризація провадиться інвентаризаційною комісією, а не окремою посадовою особою. Також зазначеними нормами визначені випадки обов'язкової інвентаризації. Інвентаризація апаратних та програмних засобів в межах щорічної інвентаризації у строки, встановлені Положенням про інвентаризацію. При цьому, відповідальна особа здійснює контроль за встановленим програмним забезпеченням в межах пп. 6 цього пункту, а не шляхом проведення інвентаризації	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис.	15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. **Надавач фінансових послуг має право об'єднувати окремі внутрішні документи з питань інформаційної безпеки та кіберзахисту в один або кілька документів, не порушуючи вимог цього Положення.** Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис.	Можливість об'єднання окремих внутрішніх документів в один або кілька документів передбачена й іншими нормативно-правовими актами НБУ, зокрема, п. 10 Положення НБУ № 15.			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
16. Надавач фінансових послуг зобов'язаний щорічно (один раз на рік з моменту останнього проведеного перегляду) переглядати внутрішні документи з питань інформаційної безпеки та кіберзахисту та оновлювати їх в разі суттєвої зміни умов функціонування інформаційно-комунікаційних систем, в яких надавач фінансових послуг при наданні послуг здійснює обробку інформації, яка віднесена до таємниці фінансової послуги.	16. Надавач фінансових послуг зобов'язаний ~~щорічно (один раз на рік з моменту останнього проведеного перегляду)~~ переглядати внутрішні документи з питань інформаційної безпеки та кіберзахисту та оновлювати їх в разі суттєвої зміни умов функціонування інформаційно-комунікаційних систем, в яких надавач фінансових послуг при наданні послуг здійснює обробку інформації, яка віднесена до таємниці фінансової послуги.	Необхідність в перегляді та оновлені документів виникає не щорічно, а тільки у випадках дійсної необхідності в цьому. В протилежному разі це буде зайвим витрачанням фінансових та людських ресурсів на процес, який не буде жодним чином впливати на діяльність фінансової установи			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
18. Надавач фінансових послуг зобов'язаний здійснювати регулярний, але не рідше одного разу на рік з моменту останнього проведеного перегляду, перегляд прав доступу клієнтів, користувачів та привілейованих користувачів до своїх інформаційно-комунікаційних систем.	18. Надавач фінансових послуг **має самостійно визначати періодичність перегляду** ~~зобов'язаний здійснювати регулярний, але не рідше одного разу на рік з моменту останнього проведеного перегляду, перегляд~~ прав доступу клієнтів, користувачів та привілейованих користувачів до своїх інформаційно-комунікаційних систем.	аналогічні вимоги визначені для банків в п. 36, 39 Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (Постанова НБУ від 28.09.2017 № 95)			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
21. Надавач фінансових послуг зобов'язаний запровадити технології та процедури безпечної автентифікації, які повинні впроваджуватися на основі відповідної політики з контролю доступу для забезпечення безпечної автентифікації клієнтів, користувачів та привілейованих користувачів при наданні доступу до інформаційно-комунікаційних систем надавача фінансових послуг.	21. Надавач фінансових послуг зобов'язаний запровадити технології та процедури безпечної автентифікації, які повинні впроваджуватися на основі **внутрішніх документів, що регламентують контроль** ~~відповідної політики~~ з ~~контролю~~ доступу для забезпечення безпечної автентифікації клієнтів, користувачів та привілейованих користувачів при наданні доступу до інформаційно-комунікаційних систем надавача фінансових послуг.	процедури автентифікації не обов'язково повинні бути регламентовані політикою. Це може бути будь-який внутрішній документ. Тим більш, що політика перш за все визначає загальні вимоги, певні межи, критерії, а не конкретизує ті чи інші процедури			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. ~~Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації.~~ ~~Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.~~	ДСТУ EN ISO/IEC 27000:2022, ДСТУ EN ISO/IEC 27001:2022, ДСТУ EN ISO/IEC 27002:2023 таких заборон та обмежень не містять			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування); 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів; 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем; 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування); 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів, **крім випадку використання облікового запису як резервного для відновлення діяльності надавача фінансових послуг**; 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем; 4) ~~завершення дії договору з клієнтом або~~ втрата клієнтом членства у кредитній спілці (для кредитних спілок).	до пп. 2) є облікові записи, які можуть використовуватися для відновлення діяльності, а їх блокування може призвести до порушення діяльності надавача фінансових послуг До пп. 4) само по собі закінчення строку договору не може призводити до блокування запису, оскільки можуть бути укладені й інші договори, договір на момент закінчення може бути ще не виконаний та інше		
27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 60 днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі **лише у випадках підозри на їх компрометацію або після відомих інцидентів безпеки** ~~не рідше одного разу на 60 днів~~. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	У сучасних стандартах кібербезпеки, зокрема в рекомендаціях Національного інституту стандартів і технологій США (NIST), відсутня вимога щодо регулярної зміни паролів через певні проміжки часу, наприклад, кожні 60 днів. NIST рекомендує змінювати паролі лише у випадках підозри на їх компрометацію або після відомих інцидентів безпеки. Зокрема, Національний інститут стандартів і технологій США (NIST) у проекті SP 800-63-4 "Digital Identity Guidelines" рекомендує відмовитися від обов'язкової періодичної зміни паролів без конкретної причини, оскільки ця практика може знижувати рівень безпеки через схильність користувачів обирати слабші паролі.	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
28. Надавач фінансових послуг зобов'язаний забезпечити маскування значення паролю при введенні його клієнтом, користувачем та привілейованим користувачем.	28. Надавач фінансових послуг зобов'язаний забезпечити **можливість** маскування значення паролю при введенні його клієнтом, користувачем та привілейованим користувачем.	клієнт повинен мати можливість відображати пароль, як це передбачається в багатьох сервісах для зручності введення	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг **за допомогою віддаленого доступу** (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	враховуючи ризики вбачається за доцільне забезпечувати ідентифікацію обладнання, яке підключено за допомогою саме віддаленого доступу, а не пудключеного до внутрішньої мережі	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше одного року з моменту архівації, якщо інше не передбачено законодавством.	34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше **трьох місяців** ~~одного року~~ з моменту архівації, якщо інше не передбачено законодавством.	Більшість надавачів фінансових послуг, в тому числі кредитні спілки мають обмежені серверні ресурси. Зберігання логів щонайменше 1 рік буде дуже дороговартісним рішенням для них	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
III. Управління кіберінцидентами та інцидентами інформаційної безпеки	III. Управління кіберінцидентами та інцидентами інформаційної безпеки	III. Управління кіберінцидентами та інцидентами інформаційної безпеки	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

38. План реагування на кіберінциденти та інциденти інформаційної безпеки повинен містити: *** 4) порядок взаємодії відповідальної особи за забезпечення виконання вимог з інформаційної безпеки та кіберзахисту з працівниками ключових та/або критичних бізнес-процесів надавача фінансових послуг під час реагування на кіберінциденти та інциденти інформаційної безпеки;	38. План реагування на кіберінциденти та інциденти інформаційної безпеки повинен містити: *** 4) порядок взаємодії відповідальної особи за забезпечення виконання вимог з інформаційної безпеки та кіберзахисту з працівниками **основних** ~~ключових~~ ~~та/або~~ ~~критичних~~ бізнес-процесів надавача фінансових послуг під час реагування на кіберінциденти та інциденти інформаційної безпеки;	проєкт Положення та інші нормативно-правові акти не містять визначення ключових або критичних бізнес-процесів. В той же час, відповідно до пп. 3 ч. 2 ст. 4 ЗУ Про основні засади забезпечення кібербезпеки України об'єктами кіберзахисту є комунікаційні системи, **які використовуються для задоволення суспільних потреб** та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу. Таким чином, вимоги цього положення повинні розповсюджуватися саме на ті інформаційні системи, **які використовуються для створення та підтримки продуктів та послуг фінансової установи** (тобто, задоволення суспільних потреб), що як в теорії та міжнародній практиці, так й в нормативно-правових актах НБУ, зокрема пп. 2 п. 2 Положення НБУ № 15, є основним бізнес-процесом.			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
39. Надавач фінансових послуг з метою оперативного реагування на кіберінциденти та забезпечення безперервності надання основних послуг зобов'язаний забезпечити взаємодію зі сторонніми постачальниками послуг та/або аутсорсерами, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем, інтернет-сервіс провайдерами. Надавач фінансових послуг зобов'язаний в договорі на отримання послуг від цих сторонніх постачальників послуг та/або договорі аутсорсінгу передбачити умови, згідно яких сторонній постачальник послуг буде взаємодіяти з надавачем фінансових послуг з питань реагування на кіберінциденти та інциденти інформаційної безпеки. Надавач фінансових послуг зобов'язаний під час дії цього договору здійснювати моніторинг подій, включаючи кіберінциденти, інциденти інформаційної безпеки, інциденти порушення безперервності діяльності, що впливають (можуть вплинути) на надання послуг.	39. Надавач фінансових послуг з метою оперативного реагування на кіберінциденти та забезпечення безперервності надання основних послуг зобов'язаний забезпечити взаємодію зі сторонніми постачальниками послуг та/або аутсорсерами, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем, інтернет-сервіс провайдерами. Надавач фінансових послуг зобов'язаний в ~~договорі на отримання послуг від цих сторонніх постачальників послуг та/або~~ договорі аутсорсінгу передбачити умови, згідно яких **аутсорсер** ~~сторонній постачальник послуг~~ буде взаємодіяти з надавачем фінансових послуг з питань реагування на кіберінциденти та інциденти інформаційної безпеки. Надавач фінансових послуг зобов'язаний під час дії цього договору здійснювати моніторинг подій, включаючи кіберінциденти, інциденти інформаційної безпеки, інциденти порушення безперервності діяльності, що впливають (можуть вплинути) на надання послуг.	Відповідно до ч. 1 ст. 638 ЦК України Договір є укладеним, якщо сторони досягли згоди з усіх істотних умов договору. Істотними умовами договору є умови про предмет договору, умови, **що визначені законом** як істотні або є необхідними для договорів даного виду, а також усі ті умови, щодо яких за заявою хоча б однієї із сторін має бути досягнуто згоди. Будь-яка інша норма цього закону, інших законодавчих актів не надає повноважень НБУ встановлювати вимоги до умов договору зі сторонніми постачальниками послуг, **крім аутсорсера**. При цьому, умови договору про надання послуг, зазвичай, встановлюються надавачами послуг, а не користувачами цих послуг. НБУ не наділений правом регулювати відносини по наданню послуг іншими суб'єктами ніж фінансові установи.		
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
40. Національний банк має право вимагати від надавача фінансових послуг надання інформації щодо реагування на кіберінциденти та інциденти інформаційної безпеки шляхом направлення запиту.	40. Національний банк має право вимагати від надавача фінансових послуг надання інформації щодо реагування на кіберінциденти та інциденти інформаційної безпеки **(у разі їх наявності)** шляхом направлення запиту.	за відсутності кіберінциденту або інциденту інформаційної безпеки надати інформацію щодо реагування на них буде неможливо			
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
44. Надавач фінансових послуг зобов'язаний здійснити розмежування інформаційно-комунікаційних систем на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.	44. Надавач фінансових послуг **може** ~~зобов'язаний~~ здійснити розмежування інформаційно-комунікаційних систем на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.	Враховуючи, що більшість надавачів фінансових послуг, в тому числі кредитних спілок є невеликими, з невеликим штатом працівників, мережа може складатися з двох-трьох комп'ютерів, що робить недоцільним її сегментацію. При цьому, виконання даних вимог потребує великих фінансових витрат, що може стати невиконуваним для невеликих установ		
			Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

45. Надавач фінансових послуг при підключенні своїх інформаційно-комунікаційних систем до мережі Інтернет або зовнішніх мереж зобов'язаний забезпечити виконання заходів мережевого захисту: 1) забезпечення взаємодії інформаційно-комунікаційних систем (її сегментів) з зовнішніми інформаційно-комунікаційними системами тільки через контрольовані точки доступу, кількість яких має бути мінімально необхідною для вирішення завдань; 2) встановлення заборони передачі інформації, що є об'єктом захисту, за межі інформаційно-комунікаційних систем при відмові (збої) функціонування засобів захисту; 3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних систем, які не використовуються, у стан "без призначення IP-адреси" (за наявності технічної можливості реалізації); 4) забезпечення захисту від атак типу "відмова в обслуговуванні" та інших відомих мережевих атак.	45. Надавач фінансових послуг при підключенні своїх інформаційно-комунікаційних систем до мережі Інтернет або зовнішніх мереж зобов'язаний забезпечити виконання заходів мережевого захисту: 1) забезпечення взаємодії інформаційно-комунікаційних систем (її сегментів) з зовнішніми інформаційно-комунікаційними системами тільки через контрольовані точки доступу, кількість яких має бути мінімально необхідною для вирішення завдань; 2) встановлення заборони передачі інформації, що є об'єктом захисту, за межі інформаційно-комунікаційних систем при відмові (збої) функціонування засобів захисту, **крім випадків, коли передача такої інформації необхідна для відновлення функціонування інформаційно-комунікаційних систем чи засобів захисту після відмови (збою)**; 3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних систем, які не використовуються, у стан "без призначення IP-адреси" (за наявності технічної можливості реалізації); 4) забезпечення захисту від атак типу "відмова в обслуговуванні" та інших відомих мережевих атак. **Надавач фінансових послуг самостійно визначає методи та засоби (технології) захисту від такого типу атак**	до пп. 2) для відновлення інформаційної системи в деяких випадках потрібно буде передання інформації до пп. 4) з огляду на затратність забезпечення такого захисту, великі фінансові установи можуть забезпечити захист самостійно. В той же час, усі інші установи, як правило, замовляють або використовують такі сервіси за рахунок потужностей провайдерів та тих хто надає інтернет канали зв'язку сервісів та мережі фінансової установи з мережею інтернет	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
46. Надавач фінансових послуг зобов'язаний забезпечити розміщення в демілітаризованій зоні інформаційно-комунікаційних систем надавача фінансових послуг, серверів та обладнання, що забезпечує функціонування сервісів (надання послуг), які відкриті для доступу клієнтів з зовнішніх мереж.	~~46. Надавач фінансових послуг зобов'язаний забезпечити розміщення в демілітаризованій зоні інформаційно-комунікаційних систем надавача фінансових послуг, серверів та обладнання, що забезпечує функціонування сервісів (надання послуг), які відкриті для доступу клієнтів з зовнішніх мереж.~~	Проєкт передбачає створення демілітаризованої зони (DMZ) для захисту внутрішньої мережі фінансової установи від зовнішніх атак. DMZ є актуальною для великих банків та компаній, які надають онлайн-банкінг, мобільні додатки та інші складні сервіси. Кредитні спілки не надають складні онлайн-фінансові послуги, не здійснюють міжнародні транзакції та не мають серверів, до яких має бути віддалений доступ клієнтів. Витрати на впровадження DMZ значні (обладнання, налаштування, супровід), але захищати в кредитній спілці фактично нічого, оскільки більшість операцій виконується офлайн або у внутрішніх, ізольованих системах.			
48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника, **крім випадку недоцільності/неможливості перейти на версію операційної системи, що підтримується,** та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	Перехід на нові операційні системи може потягти за собою зміну обладнання, на якому вони працюють, а в деяких випадках вимоги операційних систем тягнуть за собою придбання дороговартісного обладнання, що може вплинути на діяльність невеликих фінансових установ, в тому числі кредитних спілок	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53
50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.	50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника, **крім випадку недоцільності/неможливості перейти на версію прикладного програмного забезпечення, драйверів, що підтримується,**	Перехід на нове програмне забезпечення може потягти за собою зміну обладнання, на якому воно працює, а в деяких випадках вимоги програм тягнуть за собою придбання дороговартісного обладнання, що може вплинути на діяльність невеликих фінансових установ, в тому числі кредитних спілок Також, кредитна спілка може мати необхідність у використанні специфічного обладнання, для якого нові драйвери вже не випускаються	Юридична особа: Національна асоціація кредитних спілок України	ЄДРПОУ: 20064083, (unascu@unascu.org.ua)	21.03.2025 15:08:53

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
2. Надавачам фінансових послуг протягом шести місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	2. Надавачам фінансових послуг протягом вісімнадцяти місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	Пропонується перенести строки виконання вимог Постанови з 6 місяця до 18 місяців. За цей час необхідно оновити внутрішні документи з кібербезпеки і привести їх у відповідність до Постанови Національного банку, провести оцінку та обробку ризиків та впровадити ряд технічних контролів.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
10. Надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтовний підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг.	10. Надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтовний підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту, описані в цій Постанові з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг	Уточнення для уникнення сумнівів щодо формулювання: Кожна установа, надавач фінансових послуг самостійно визначає перелік заходів забезпечення кібербезпеки та інформаційної безпеки цього Положення, які будуть впроваджені, спираючись на результати аналізу ризиків кібербезпеки.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис.	15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис або вінші спосіб, що забезпечує підтвердження ознайомлення	Пропонується додати альтернативні методи ознайомлення з внутрішніми нормативними документами з кібербезпеки та інформаційної безпеки у зв'язку запровадженням гібридного або віддаленого формату роботи.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг може використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	Уточнення для уникнення сумнівів щодо формулювання щодо багатофакторної автентифікації.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 60 днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 90 днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	Пропонується змінювати паролі не рідше одного разу на 90 днів з метою зменшення ситуацій використання схожих паролей в інформаційних системах фінансової установи.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	Видалити або спростити вимогу	Пропонується значно спростити або видалити вимоги щодо автентифікації пристроїв в мережах фінансових установ у випадках, коли внутрішні додатки фінансової установи потребують посиленої автентифікації користувача відповідно до вимог цієї Постанови.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54

34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше одного року з моменту архівації, якщо інше не передбачено законодавством.	34. Надавач фінансових послуг зобов'язаний проводити періодичне архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше 3 місяців з моменту архівації, якщо інше не передбачено законодавством. Журнали реєстрації подій пов'язані з інцидентами кібер безпеки повинні зберігатись протягом одного року.	Пропонується зменшити строк зберігання та архівування журналів реєстрації подій до 3 місяців, а журнали реєстрації подій, пов'язані з інцидентами кібер безпеки зберігати 1 рік або більше.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
45. Надавач фінансових послуг при підключенні своїх інформаційно-комунікаційних систем до мережі Інтернет або зовнішніх мереж зобов'язаний забезпечити виконання заходів мережевого захисту: 3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних систем, які не використовуються, у стан "без призначення IP-адреси" (за наявності технічної можливості реалізації);	45. Надавач фінансових послуг при підключенні своїх інформаційно-комунікаційних систем до мережі Інтернет або зовнішніх мереж зобов'язаний забезпечити виконання заходів мережевого захисту: 3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних систем, які не використовуються, у стан "відключено" (за наявності технічної можливості реалізації);	Уточнення для уникнення сумнівів щодо формулювання	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою. У випадку використання операційних систем, для яких припинено підтримку виробника, надавач фінансових послуг зобов'язаний впровадити додаткові компенсуючі заходи та провести аналіз ризиків, що включає: 1) впровадження додаткових заходів безпеки для захисту даних та системи від потенційних загроз; 2) регулярний моніторинг та аудит безпеки для виявлення та усунення вразливостей; 3) забезпечення резервного копіювання даних та плану відновлення у випадку інцидентів; 4) документування та затвердження результатів аналізу ризиків відповідно до внутрішніх політик та процедур.	Пропонується додати ріск-орієнтований підхід щодо використання операційних систем надавачами фінансових послуг.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54
50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.	50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника. У випадку використання прикладного програмного забезпечення, для якого припинено підтримку виробника, надавач фінансових послуг зобов'язаний впровадити додаткові компенсуючі заходи та провести аналіз ризиків, що включає: 1) впровадження додаткових заходів безпеки для захисту даних та системи від потенційних загроз; 2) регулярний моніторинг та аудит безпеки для виявлення та усунення вразливостей; 3) забезпечення резервного копіювання даних та плану відновлення у випадку інцидентів; 4) документування та затвердження результатів аналізу ризиків відповідно до внутрішніх політик та процедур.	Пропонується додати ріск-орієнтований підхід щодо використання програмного забезпечення надавачами фінансових послуг.	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54

24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування); 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів; 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем; 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування на обмежений період часу); 2) відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 45 календарних днів (за винятком випадків, коли це було розглянуто при аналізі ризиків та впроваджено відповідні компенсуючі заходи); 3) звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем; 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	Пропонується додати ріск-орієнтований підхід щодо блокування облікових записів при відсутності авторизації користувача. Зменшення строку відсутності авторизації користувача до 45 календарних днів або відобразити в нормі Постанови: «90 або менше календарних днів».	Юридична особа: ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО СТРАХОВА КОМПАНІЯ АРКС	ЄДРПОУ: 20474912, (serhii.bozhok@arx.com.ua)	23.03.2025 23:15:54

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
п.21. Надавач фінансових послуг зобов'язаний запровадити технології та процедури безпечної автентифікації, які повинні впроваджуватися на основі відповідної політики з контролю доступу для забезпечення безпечної автентифікації клієнтів, користувачів та привілейованих користувачів при наданні доступу до інформаційно-комунікаційних систем надавача фінансових послуг.	**Додати в п.2 Терміни в цьому Положенні вживаються в таких значеннях опис «процедури безпечної автентифікації»**	Відсутність визначеного терміну дозволяє кожному учаснику трактувати це на власний розсуд	Юридична особа: ПрАТ "СК "ВУСО"	ЄДРПОУ: 31650052, (bondarenko.av@vuso.ua)	24.03.2025 14:54:18
п.23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	Викласти в наступній редакції п.23. Надавач фінансових послуг може використовувати біометрію як частину багатофакторної автентифікації.	Другим фактором може бути Майкрософт аутентифікатор, який при вході використовує біометрію але як другий фактор код.	Юридична особа: ПрАТ "СК "ВУСО"	ЄДРПОУ: 31650052, (bondarenko.av@vuso.ua)	24.03.2025 14:54:18
п.27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 60 днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	Викласти в наступній редакції п.27 Користувачі та привілейовані користувачі зобов'язані змінювати паролі одразу після компрометації.	NIST (National Institute of Standards and Technology): Recommends changing passwords only if compromised, but privileged accounts may need stricter controls. Майкрософт: Don't require mandatory periodic password resets for user accounts https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide	Юридична особа: ПрАТ "СК "ВУСО"	ЄДРПОУ: 31650052, (bondarenko.av@vuso.ua)	24.03.2025 14:54:18
п.32 Надавач фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг в спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події.....	Викласти в наступній редакції п.32 Надавач фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг в спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події по критично важливих системах.	Логувати все про всіх це суттєво та необґрунтовано збільшує витрати на збір та збереження даних для Компанії.	Юридична особа: ПрАТ "СК "ВУСО"	ЄДРПОУ: 31650052, (bondarenko.av@vuso.ua)	24.03.2025 14:54:18

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
15. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис.	15. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис **(в електронній чи паперовій формі)**.	В страховика наявна велика кількість користувачів (штатні працівники, залучені агенти). У разі впровадження, необхідно буде друкувати пакет документів та надавати для **фізичного підписання** як штатним працівникам, так і **кожному Агенту (ФОП)**, з подальшою **відправкою** підписаного пакету документів до Головного офісу компанії і **зберіганням** паперових документів в Головному офісі. Для існуючих користувачів (в т.ч. Агентів) - потрібно буде провести підписання пакету документів, **доставку** та зберігання у Головному офісі компанії. Введення можливості підписання в електронному вигляді дозволить оптимізувати та спростити процес підписання, зберігання інформації тощо.	Юридична особа: Княжа Вієнна Іншуранс Груп	ЄДРПОУ: 24175269, (reception@kniazha.ua)	24.03.2025 18:01:46
23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг.	23. Надавач фінансових послуг **має право** запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг.	У разі впровадження, при **кожному** вході **кожного** користувача, в інформаційно-комунікаційну систему, буде відбуватись відправка SMS кожному користувачу. Таке направлення SMS потребуватиме додаткових витрат, обслуговуванні яга розширенян штату. Додатково з'являється **залежність роботи Системи Компанії від роботи стороннього сервісу відправок SMS** (TurboSMS, SMSClub).	Юридична особа: Княжа Вієнна Іншуранс Груп	ЄДРПОУ: 24175269, (reception@kniazha.ua)	24.03.2025 18:01:46
27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 60 днів.	видалити п. 27	Зміна пароля кожні 60 днів (фактично - менше, т.я. нагадування про зміну буде приходити за 2 тижні) - призведе до того, що Користувачі будуть забувати нові паролі або записувати їх на папері біля ПК - що тільки погіршить безпекову ситуацію, збільшиться кількість "заблокованих користувачів" та час на їх розблокування. Все це може вплинути на ефективність роботи та безпеку. Просимо врахувати, що Міжнародний стандарт IT - ISO 27001 не вимагає періодичної зміни паролей у випадку використання складних паролей: Мінімум 12 символів, великі, маленькі букви, цифри, символи. Наголос робиться на складності пароля, а не на частоті зміни. Велика частота зміни пароля призводить до того, що користувачі використовують слабкі паролі, вимушені записувати їх та часто забувають.	Юридична особа: Княжа Вієнна Іншуранс Груп	ЄДРПОУ: 24175269, (reception@kniazha.ua)	24.03.2025 18:01:46
31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації, **за виключенням випадків коли інформаційно-комунікаційна система страховика працює в хмарі і доступ до інформаційно-комунікаційної системи здійснюється через веб сервер, що розташований в окремому сегменті мережі.**	Просимо розглянути в положенні випадок коли обладнання зовнішнього користувача не підключається і не має доступу до внутніших ресурсів Мережі. З урахуванням того факту, що інформаційно-комунікаційна система страховика може фізично працювати в хмарі Microsoft Azure, AWS і т.д. і доступ до системи відбувається через ВЕБ сервер, розташований в окремому сегменті мережі - яким чином дана вимога посилює захист?	Юридична особа: Княжа Вієнна Іншуранс Груп	ЄДРПОУ: 24175269, (reception@kniazha.ua)	24.03.2025 18:01:46
45.4) забезпечення захисту від атак типу "відмова в обслуговуванні"		Просимо уточнити в положенні перелік систем, що забезпечують захист від атак типу "відмова в обслуговуванні"	Юридична особа: Княжа Вієнна Іншуранс Груп	ЄДРПОУ: 24175269, (reception@kniazha.ua)	24.03.2025 18:01:46

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 1) забезпечує виконання вимог з інформаційної безпеки та кіберзахисту, що встановлені цим Положенням; 2) розробляє політику інформаційної безпеки відповідно до вимог цього Положення; 3) організовує регулярну, **але не рідше одного разу на рік з моменту останньої проведеної інвентаризації**, інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг;	14. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг: 1) забезпечує виконання вимог з інформаційної безпеки та кіберзахисту, що встановлені цим Положенням; 2) розробляє політику інформаційної безпеки відповідно до вимог цього Положення; 3) організовує регулярну інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг **у порядку, визначеному внутрішніми документами**;	Постійна інвентаризація, без адаптації до діяльності надавача фінансових послуг, та в разі відсутності змін у діяльності - створює тільки додаткове навантаження на організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12
Пункт 23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг **повинен** використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	Пункт 23 викласти в такій редакції: Надавач фінансових послуг зобов'язаний запровадити та використовувати **автентифікаціюдля користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг, відповідно до вимог його внутрішніх документів, яка б дозволяла забезпечечити** багатофакторну (множинну) автентифікацію . ... Надавач фінансових послуг **може** використовувати біометрію як фактор автентифікації як частину багатофакторної автентифікації.	Надавач фінансових послуг, що має ліцензію на здійснення валютних операцій в частині торгівлі валютними цінностями в готівковій формі, не зберігає інформації про клієнта, яка б містила таємницю фінансової послуги, окрім як відеозапису щодо здійснення операцій клієнтом, яка видаляється через 14 діб та інформації, отриманої за процедурою здійснення фінансового моніторингу, тому обов'язок використовувати біометрію як фактор автентифікації як частину багатофакторної автентифікації є недоцільним.	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12
Пункт 34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання **не менше одного року з моменту архівації**, якщо інше не передбачено законодавством.	Пункт 23 викласти в такій редакції: Надавач фінансових послуг зобов'язаний проводити періодичне, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання, **в строки встановлені у внутрішніх документах надавача фінансових послу**г, якщо інше не передбачено законодавством.	Надавач фінансових послуг може самостійно визначати необхідність періодичність архівування та строки зберігання журналів реєстрації подій (логи). Зберігання не менше одного року може бути тяжким для виконання, оскільки міститиме великий об'єм інформації.	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12
Пункт 48 Надавач фінансових послуг зобов'язаний використовувати операційні системи, **для яких не припинено підтримку виробника та** які забезпечують можливість: 1) Ідентифікації та автентифікації всіх користувачів операційної системи; 2) Розмежування доступу користувачів операційної системи; 3) Реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	Пункт 48 викласти в такій редакції: Надавач фінансових послуг зобов'язаний використовувати **операційні системи, крім тих, які обслуговуються державою-агресором, які забезпечують можливість:** 1) Ідентифікації та автентифікації всіх користувачів операційної системи; 2) Розмежування доступу користувачів операційної системи; 3) Реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	Використання операційних систем, в яких припинено підтримку виробника, не означає що ПЗ працює неефективно, або є ризик його використання у злочинних цілях, більш ніж ОС та/або не виконує належні йому функції.	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12
39. Надавач фінансових послуг з метою оперативного реагування на кіберінциденти та забезпечення безперервності надання основних послуг **зобов'язаний забезпечити** взаємодію зі сторонніми постачальниками послуг та/або аутсорсерами, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем, інтернет-сервіс провайдерами.	39. Надавач фінансових послуг з метою оперативного реагування на кіберінциденти та забезпечення безперервності надання основних послуг **, в разі необхідності, взаємодіє** зі сторонніми постачальниками послуг та/або аутсорсерами, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем, інтернет-сервіс провайдерами.	Може застосовуватись тільки в разі наявності такої взаємодії.	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12

Пункт 50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, **для яких не припинено підтримку виробника.**	Пункт 50 викласти в такій редакції: Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів. Також просимо розяснити, що саме відноситься до прикладного програмного забезпечення.	Використання програмного забезпечення, в якого припинено підтримку виробника, не означає що таке ПЗ працює неефективно, та/або не виконує належні йому функції. Окрім того, є ряд юридичних осіб, окрім виробника, які можуть підтримувати певне програмне забезпечення.	Юридична особа: Приватне акціонерне товариство "Українська фінансова група"	ЄДРПОУ: 14285934, (ufg@ufg.com.ua)	24.03.2025 18:18:12

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
2. Надавачам фінансових послуг протягом шести місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	2. Надавачам фінансових послуг протягом ~~шести~~ **дванадцяти** місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	Оскільки проєкт передбачає необхідні, актуальні та підтримувані страховиками зміни до процесу організації інформаційної безпеки, які у той же час передбачають необхідність вибору рішення, його тестування, та впровадження, складення та реалізацію бюджету витрат, запропонований строк у 6 місяців видається страховиками вкрай замалим.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту під підпис.	15. Надавач фінансових послуг зобов'язаний ознайомити користувачів та привілейованих користувачів з внутрішніми документами з питань інформаційної безпеки та кіберзахисту**, що необхідні для виконання їх службових обов'язків**. Внутрішні документи з питань інформаційної безпеки та кіберзахисту розробляються надавачем фінансових послуг з урахуванням вимог цього Положення. Перелік внутрішніх документів з питань інформаційної безпеки та кіберзахисту для ознайомлення визначається надавачем фінансових послуг самостійно, з урахуванням принципу мінімальної достатності для досягнення мети і завдань з питань інформаційної безпеки та кіберзахисту. Користувач та привілейований користувач зобов'язані ознайомитися з внутрішніми документами з питань інформаційної безпеки та кіберзахисту ~~під підпис~~ **в спосіб, що дає змогу підтвердити факт та дату такого ознайомлення, включаючи надання внутрішніх документів для ознайомлення засобами електронної пошти або ознайомлення під підпис працівника та особи, яка забезпечила проведення ознайомлення.**	Враховуючи вже визначені іншими нормативно-правовими актами НБУ можливості та вимоги до ознайомлення працівників із внутрішніми документами страховика, та вже впроваджені страховиками інструменти такого ознайомлення, що є значно ширшими, втім забезпечують можливість підтвердження факту ознайомлення, вимога ознайомлення виключно «під підпис» видається невиправданою.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. Надавач фінансових послуг повинен використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	23. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів при здійсненні ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг. Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації. **ВИДАЛИТИ або ВІДТЕРМІНУВАТИ** або викласти в такій редакції Надавач фінансових послуг ~~повинен~~ **має право** використовувати біометрію як фактор автентифікації лише як частину багатофакторної автентифікації.	Через відсутність в процесах страховка реальної потреби у використанні біометрії як фактору автентифікації, пропонується виключити таку вимогу або залишити її опціонною на розсуд страховика. У разі, якщо така вимога залишатиметься у проєкті, пропонуєтся визначити її застосування при здійсненні віддаленого доступу тільки до тих інформаційно-комунікаційних систем, що доступні за межами внутрішньої корпоративної мережі надавача фінансових послуг. Також в разі залишення вимоги про обов'язковість застосування біометрії просимо відтермінувати її запровадження через технічну складність реалізації.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 2)відсутності авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів;	24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 2)відсутності авторизації ~~користувача,~~ привілейованого користувача в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів;	користувачі, серед яких можуть бути страхові посередники, можуть не користуватися обліковим записом понад 90 днів відповідно до бізнес-процесів страховика. Тобто відсутність активності у такий строк є нормальним для діяльності страховиків, і обов'язкове блокування негативно вплине та їх діяльність.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38

24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 3)звільнення користувача, привілейованого користувача або зміна статусу користувача, привілейованого користувача , який не передбачає доступу до цих систем;	24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 3)відсутня редакція змін ;	норма потребує уточнення оскільки не має однакового розуміння. Зокрема, "звільнення користувача" (працівника?), "статус користувача" (статус користувачів та привілейований користувач?) , чи розповсюджується норма на сторонніх підрядників, тощо	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 4) завершення дії договору з клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	24. Надавач фінансових послуг зобов'язаний забезпечити блокування облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг в таких випадках: 4) завершення дії договору з клієнтом **(крім страховиків)** або втрата клієнтом членства у кредитній спілці (для кредитних спілок).	Передбачене проєктом блокування користувачів при спливі строку дії договору для страховиків є невиправданим, оскільки не враховує використанні облікових записів для потреб врегулювання, що відбувається після закінчення дії договорів.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на 60 днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	27. Користувачі та привілейовані користувачі зобов'язані змінювати паролі не рідше одного разу на ~~60~~ **90** днів. При цьому повторення вибраного складного паролю може здійснюватися не менш ніж на восьмий раз.	Примусова зміна паролів у 60 днів не тільки здатна негативно вплинути на окремі процеси страховка, а також в окремих випадках не відповідає політикам груп, до яких входять страховики, та створить складнощі у їх діяльності.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
10. Надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтовний підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг.	10. Надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтовний підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту, описані в цій Постанові з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг.	Пропозиція СК АРКС Уточнення для уникнення сумнівів щодо формулювання: Кожна установа, надавач фінансових послуг самостійно визначає перелік заходів забезпечення кібербезпеки та інформаційної безпеки цього Положення, які будуть впровадження, спираючись на результати аналізу ризиків кібербезпеки.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
34. Надавач фінансових послуг зобов'язаний проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування, архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше одного року з моменту архівації, якщо інше не передбачено законодавством.	34. Надавач фінансових послуг зобов'язаний проводити періодичне архівування журналів реєстрації подій (логи) та забезпечити їх зберігання не менше 3 місяців з моменту архівації, якщо інше не передбачено законодавством. Журнали реєстрації подій пов'язані з інцидентами кібер безпеки повинні зберігатись протягом одного року.	Пропозиція СК АРКС Пропонується зменшити строк зберігання та архівування журналів реєстрації подій до 3 місяців, а журнали реєстрації подій, пов'язані з інцидентами кібер безпеки зберігати 1 рік або більше.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою.	48. Надавач фінансових послуг зобов'язаний використовувати операційні системи, для яких не припинено підтримку виробника та які забезпечують можливість: 1) ідентифікації та автентифікації всіх користувачів операційної системи; 2) розмежування доступу користувачів операційної системи; 3) реєстрації дій, що виконуються користувачами операційної системи та самою операційною системою. **У випадку використання операційних систем, для яких припинено підтримку виробника, надавач фінансових послуг зобов'язаний впровадити додаткові компенсуючі заходи та провести аналіз ризиків, що включає:** **1) впровадження додаткових заходів безпеки для захисту даних та системи від потенційних загроз;** **2) регулярний моніторинг та аудит безпеки для виявлення та усунення вразливостей;** **3) забезпечення резервного копіювання даних та плану відновлення у випадку інцидентів;** **4) документування та затвердження результатів аналізу ризиків відповідно до внутрішніх політик та процедур.**	Пропозиція СК АРКС Пропонується додати ризик-орієнтований підхід щодо використання операційних систем надавачами фінансових послуг.	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38

50. Надавач фінансових послуг зобов’язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.	50. Надавач фінансових послуг зобов’язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника. **У випадку використання прикладного програмного забезпечення, для якого припинено підтримку виробника, надавач фінансових послуг зобов’язаний впровадити додаткові компенсуючі заходи та провести аналіз ризиків, що включає:** **1)впровадження додаткових заходів безпеки для захисту даних та системи від потенційних загроз;** **2)регулярний моніторинг та аудит безпеки для виявлення та усунення вразливостей;** **3)забезпечення резервного копіювання даних та плану відновлення у випадку інцидентів;** **4)документування та затвердження результатів аналізу ризиків відповідно до внутрішніх політик та процедур.**	Пропозиція СК АРКС Пропонується додати ризик-орієнтований підхід щодо використання програмного забезпечення надавачами фінансових послуг.			
«Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг»	інші пропозиції щодо надання визначень окремих термінів та унормування з вимогами іних положень цього проєкту та інших НПА НБУ	надано в листі НАСУ №2-353 від 21.03.2025 року	Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38
			Юридична особа: АСОЦІАЦІЯ "НАЦІОНАЛЬНА АСОЦІАЦІЯ СТРАХОВИКІВ УКРАЇНИ"	ЄДРПОУ: 41697701, (office@nasu.com.ua)	24.03.2025 19:19:38

Ви переглядаєте подані до Національного банку зауваження і пропозиції до проєкту нормативно-правового акта від заінтересованих осіб.
Національний банк не несе відповідальності за зміст інформації, викладеної заінтересованими особами. Національний банк не може бути притягнутий до відповідальності за таку інформацію.

Норма оприлюдненого проєкту акта Національного банку України (зазначається структурна одиниця проєкту акта, до якого надаються зауваження та пропозиції та текст норми проєкту акта)	Зауваження і пропозиції заінтересованих осіб	Обґрунтування зауважень і пропозицій заінтересованих осіб	Найменування юридичної особи / прізвище, власне ім'я, по батькові фізичної особи, яка надала зауваження і пропозиції	Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України, електронна пошта юридичної особи / електронна пошта фізичної особи	Дата і час подання
пункт 2 проєкту Постанови: 2. Надавачам фінансових послуг протягом **шести** місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	**пункт 2 проєкту Постанови:** 2. Надавачам фінансових послуг протягом **дванадцяти** місяців із дня набрання чинності цієї постановою привести свою діяльність у відповідність до вимог Положення.	Термін впровадження систем, необхідних для виконання запропонованих вимог проєкту Положення, більший за 6 місяців.	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 3 пункту 14 проєкту Положення: 3) організовує регулярну, але не рідше одного разу на рік з моменту останньої проведеної інвентаризації, інвентаризацію програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг;	**підпункт 3 пункту 14 проєкту Положення:** 3) організує регулярний, але не рідше одного разу на рік, з моменту останньої проведеної інвентаризації, **контроль результатів** інвентаризації програмних та апаратних засобів інформаційно-комунікаційних систем надавача фінансових послуг	Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки не закуповує, не вводить в експлуатацію програмні та апаратні засоби, облік здійснює підрозділ ІТ, адміністративно-господарський відділ, тощо, відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки повинна перевіряти результати інвентаризації	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 5 пункту 14 проєкту Положення: 5) **організовує** контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг та забезпечують **відновлення** їх працездатності в разі порушення штатного режиму функціонування;	**підпункт 5 пункту 14 проєкту Положення: 5) Здійснює** контроль за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах надавача фінансових послуг, а також забезпечує **контроль** за відновленням їх працездатності у разі порушення штатного режиму функціонування	Технічне забезпечення та відновлення здійснює підрозділ ІТ та/або підрядники. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту здійснює контроль	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 6 пункту 14 проєкту Положення: 6) уживає заходів щодо недопущення встановлення та використання в складі інформаційно-комунікаційних систем програмних і апаратних засобів, що не передбачені внутрішніми документами надавача фінансових послуг;	**підпункт 6 пункту 14 проєкту Положення: 6) Здійснює контроль** щодо недопущення встановлення та використання у складі інформаційно-комунікаційних систем програмних і апаратних засобів, не передбачених внутрішніми документами надавача фінансових послуг	Уживає заходи щодо недопущення встановлення - підрозділ ІТ. Відповідальна особа за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту - здійснює контроль	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
абзац 2 пункту 23 проєкту Положення: Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації.	**абзац 2 пункту 23 проєкту Положення:** ~~Надавачу фінансових послуг забороняється використання електронної пошти як каналу для багатофакторної автентифікації.~~	Пропонуємо вилучити. Відповідно до даних сайту Державної служби спеціального зв'язку та захисту інформації України - Додатковим фактором для перевірки може бути підтвердження: ▪ через код, надісланий у смс; ▪ через дзвінок на мобільний; ▪ через лист на e-mail; ▪ через надсилання сповіщення – така можливість, наприклад, є для акаунтів Google; ▪ через код, згенерований за допомогою спеціальних мобільних додатків (наприклад, Google Authenticator, Microsoft Authentificator чи інші) тощо. https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 1 пункту 24 проєкту Положення: 1) п'яти невдалих спроб автентифікації поспіль (автоматичне блокування);	**підпункт 1 пункту 24 проєкту Положення:** 1)п'яти невдалих спроб автентифікації поспіль (автоматичне, **тимчасове або постійне** блокування**)**	Відповідно до ISO/IEC 27001, 27002 рекомендується блокування після кількох (зазвичай 3-5) невдалих спроб та застосування механізму розблокування (автоматично через N хвилин або через службу підтримки).	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 2 пункту 24 проєкту Положення: 2) відсутності авторизації користувача, **привілейованого користувача** в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів;	**підпункт 2 пункту 24 проєкту Положення:** 2)відсутності авторизації **внутрішнього** користувача (**штатного співробітника або страхового посередника)** в інформаційно-комунікаційних системах надавача фінансових послуг протягом 90 календарних днів	блокування привілейованого користувача в інформаційно-комунікаційних системах може заблокувати можливість адміністрування ІКС	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 3 пункту 24 проєкту Положення: 3) звільнення користувача, привілейованого користувача або зміна **статусу користувача, привілейованого користувача**, який не передбачає доступу до цих систем;	**підпункт 3 пункту 24 проєкту Положення:** 3)звільнення користувача, привілейованого користувача або зміна **функціональних обов'язків**, які не передбачають доступу до цих систем	термін «функціональні обов'язки» більш визначений ніж термін «статус»	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
підпункт 4 пункту 24 проєкту Положення: 4) завершення дії договору з **клієнтом або втрата клієнтом членства у кредитній спілці (для кредитних спілок).**	**підпункт 4 пункту 24 проєкту Положення:** 4)завершення дії договору **з підрядником, якому надавався доступ до інформаційно-комунікаційних системах надавача фінансових послуг**	Клієнтам надається доступ до кабінетів сайту та мобільного додатку надавача і не доречно їх блокувати після закінчення короткострокового договору, для можливості укладання нового	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
пункт 26 проєкту Положення: 26. Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менш ніж 12 символів та містять цифри, букви в різних регістрах та спеціальні символи.	**пункт 26 проєкту Положення:** 26. Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менш ніж 12 символів та містять цифри, букви в різних регістрах та спеціальні символи **(при умові, що система підтримує спеціальні символи).**	Не кожна система підтримує введення спеціальних символів для паролів	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59

пункт 29 проєкту Положення: 29. Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування облікових записів **привілейованих користувачів** інформаційно-комунікаційних систем, що встановлюються за замовчуванням (за наявності технічної можливості та за умови збереження функціонування інформаційно-комунікаційних систем), та відключення гостьових облікових записів.	**пункт 29 проєкту Положення: 29.** Надавач фінансових послуг зобов'язаний забезпечити блокування або перейменування **стандартних адміністративних** облікових записів інформаційно-комунікаційних систем, що встановлюються за замовчуванням (за наявності технічної можливості та за умови збереження функціонування інформаційно-комунікаційних систем), та відключення гостьових облікових записів.	якщо мова йде про стандартний адміністративний обліковий запис – вважаємо за доцільне замінити на нього термін «облікових записів привілейованих користувачів інформаційно-комунікаційних систем, що встановлюються за замовчуванням»	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
пункт 31 проєкту Положення: 31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.	**пункт 31 проєкту Положення:** 31. Надавач фінансових послуг зобов'язаний забезпечити ідентифікацію обладнання **користувачів** персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем надавача фінансових послуг (за ідентифікатором управління доступом до обладнання, MAC-адресою), та запровадити заходи, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації. **Надавач фінансових послуг має право самостійно визначати перелік користувачів, для яких необхідно забезпечувати ідентифікацію обладнання за ідентифікатором управління доступом до обладнання, MAC-адресою.**	Це не повинно застосовуватись до обладнання клієнтів надавача фінансових послуг, оскільки на сучасних пристроях встановлена функція рандомізації MAC-адреси і ми не можемо унеможливлювати роботу клієнта якщо він підключається до ІКС надавача фінансових послуг з нової MAC-адреси. Оскільки відповідно до 8-10 пунктів надавач фінансових послуг має право самостійно визначати підходи (методики) оцінювання та оброблення кіберризиків та ризиків інформаційної безпеки, то вважаємо за необхідне також надати йому право самостійно визначати перелік користувачів, обладнання яких потребує ідентифікації (технічно частина користувачів, яка проходить багатофакторну ідентифікацію, працює через веб сервіси, можливості яких є обмеженими, а ідентифікація обладнання таких користувачів є надмірною та непотрібною)	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
пункт 50 проєкту Положення: 50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника.	**пункт 50 проєкту Положення:** 50. Надавач фінансових послуг зобов'язаний використовувати офіційні версії прикладного програмного забезпечення та драйверів, для яких не припинено підтримку виробника, **та/або програмне забезпечення, розроблене для надавача відповідно укладених договорів постачання програмного забезпечення. У випадках, коли надавач фінансових послуг є власником інтелектуальних та/або майнових прав на прикладне програмне забезпечення, він може самостійно здійснювати доопрацювання, випуск нових офіційних версій та підтримку даного прикладного програмного забезпечення.**	Якщо Надавач фінансових послуг викупив у розробника програмний продукт і здійснює підтримку програмного продукту силами штатних спеціалістів, що в такому випадку?	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59
Відсутній	**Оскільки певні існуючі інформаційні системи страховика можуть бути не сумісними для реалізації всіх зазначених в проекті вимог та функцій, пропонуємо передбачити механізм, коли страховик може заявити, що окрема вимога чи функція не може бути реалізована в його інформаційній системі, та проінформувати НБУ, яким альтернативним способом вирішується проблема, яку мали забезпечити дана вимога чи функція.**	Пропонуємо передбачити таку можливість	Юридична особа: Ліга страхових організацій України	ЄДРПОУ: 19478514, (liga@uainsur.com)	24.03.2025 20:13:59