Офіційно опубліковано 12.12.2025

Правління Національного банку України

П О С Т А Н О В А

09 грудня 2025 року Київ № 143

Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 5, 10 Закону України “Про фінансові послуги та фінансові компанії”, статті 113 Закону України “Про страхування”, з метою встановлення для надавачів фінансових послуг вимог щодо інформаційної безпеки та кіберзахисту на ринках фінансових послуг Правління Національного банку України **постановляє:**

1. Затвердити Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг (далі – Положення), що додається.

2. Надавачам фінансових послуг протягом 12 місяців із дня набрання чинності цією постановою привести свою діяльність у відповідність до вимог Положення.

3. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома надавачів фінансових послуг інформацію про прийняття цієї постанови.

4. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

5. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування.

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
09 грудня 2025 року № 143

Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про фінансові послуги та фінансові компанії" (далі – Закон про фінансові послуги), "Про страхування", "Про захист інформації в інформаційно-комунікаційних системах" (далі – Закон про захист інформації), "Про основні засади забезпечення кібербезпеки України" (далі – Закон про забезпечення кібербезпеки) з урахуванням Регламенту (ЄС) 2022/2554 Європейського парламенту та Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектору та внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909/2014 та (ЄС) 2016/1011, національного стандарту України ДСТУ EN ISO/IEC 27000:2022 "Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів", прийнятого наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 28 грудня 2022 року № 285 (зі змінами), національного стандарту ДСТУ ISO/IEC 27001:2023 "Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги", прийнятого наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 17 серпня 2023 року № 210 (зі змінами), національного стандарту ДСТУ ISO/IEC 27002:2023 "Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки", прийнятого наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 17 серпня 2023 року № 210 (зі змінами), з метою організації заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг та визначає порядок, базові вимоги та заходи щодо забезпечення інформаційної безпеки та кіберзахисту для таких надавачів фінансових послуг, як небанківські фінансові установи (далі – надавач фінансових послуг):

1) страховиків;

2) кредитних спілок;

3) фінансових компаній;

4) ломбардів.

2. Терміни в цьому Положенні вживаються в такому значенні:

1) внутрішні документи – документи, затверджені керівником або органом управління надавача фінансових послуг у межах його компетенції;

2) гостьовий обліковий запис – обліковий запис з обмеженим доступом, створений для тимчасового використання особами з визначеними правами, терміном дії та аудитом усіх дій;

3) зона мережі з підвищеним рівнем безпеки – 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) інцидент інформаційної безпеки – подія або низка несприятливих подій інформаційної безпеки, які можуть призвести до збитків і втрат надавача фінансових послуг або поставити під загрозу конфіденційність, цілісність та доступність інформації надавача фінансових послуг;

5) кіберризик – ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз, є складовою ризику інформаційної безпеки;

6) користувач – працівник надавача фінансових послуг, надавача супровідних послуг, аутсорсера, іншої особи, який отримав право доступу до інформаційно-комунікаційних систем надавача фінансових послуг для виконання покладених на нього функцій та завдань;

7) основні бізнес-процеси – сукупність взаємопов’язаних або взаємодіючих видів діяльності, включаючи функції, передані на аутсорсинг, спрямованих на створення певного продукту або послуги, дії, операції, завдання, що виконуються структурними підрозділами, окремими працівниками надавача фінансових послуг, інформаційними системами, 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 суттєвих збитків надавачу фінансових послуг або його користувачам та/або може призвести до порушення вимог законодавства України;

8) привілейований користувач – користувач, якому надавачем фінансових послуг надані права доступу, що перевищують права доступу користувачів й пов’язані з виконанням функцій розроблення, адміністрування, технічної підтримки інформаційно-комунікаційних систем надавача фінансових послуг;

9) ризик-орієнтований підхід – прийняття управлінських рішень щодо впровадження заходів з інформаційної безпеки та кіберзахисту на підставі аналізу порівняння поточних ризиків інформаційної безпеки і кіберризиків з прийнятними;

10) управління правами доступу до інформаційно-комунікаційних систем надавача фінансових послуг – встановлений та затверджений надавачем фінансових послуг порядок використання, реєстрації, надання, скасування, перегляду та контролю доступу до інформаційно-комунікаційних систем надавача фінансових послуг.

Термін “керівник” уживається в цьому Положенні в значенні, наведеному в Положенні про авторизацію надавачів фінансових послуг та умови здійснення ними діяльності з надання фінансових послуг, затвердженому постановою Правління Національного банку України від 29 грудня 2023 року № 199 (зі змінами).

Термін “інцидент кібербезпеки” уживається в цьому Положенні в значенні, наведеному в Законі про забезпечення кібербезпеки.

Термін “клієнт” уживається в цьому Положенні в значенні, наведеному в Законі про фінансові послуги.

Інші терміни в цьому Положенні вживаються у значеннях, наведених у Законі про фінансові послуги, Законі про захист інформації, Законі про забезпечення кібербезпеки, Законі України “Про страхування” та нормативно-правових актах Національного банку з питань регулювання діяльності надавачів фінансових послуг.

3. Вимоги цього Положення поширюються на надавачів фінансових послуг з урахуванням пункту 103 глави 12 та глави 13 розділу III Положення про вимоги до системи управління страховика, затвердженого постановою Правління Національного банку України від 27 грудня 2023 року № 194 (зі змінами), пунктів 18, 21, 27 розділу III та розділу IV Положення про порядок обліку страховиком договорів, пов’язаних зі здійсненням діяльності із страхування, та вимоги до захисту інформації страховика, затвердженого постановою Правління Національного банку України від 29 грудня 2023 року № 204 (зі змінами) (далі – Положення № 204), пунктів 136 та 137 глави 13, пункту 149 глави 14 розділу III, глави 21 розділу IV Положення про вимоги до системи управління кредитною спілкою, затвердженого постановою Правління Національного банку України від 02 лютого 2024 року № 15 (зі змінами), глави 18 розділу VI Положення про вимоги до системи корпоративного управління та системи внутрішнього контролю фінансової компанії, затвердженого

постановою Правління Національного банку України від 27 грудня 2024 року № 185 (зі змінами).

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.

5. Надавач фінансових послуг зобов'язаний вживати заходів із забезпечення інформаційної безпеки та кіберзахисту до об'єктів захисту, що встановлені цим Положенням, якими є:

1) інформація, що становить таємницю страхування, яка обробляється в інформаційно-комунікаційних системах страховика (перестраховика) або страхового посередника у зв'язку з укладенням та/або виконанням договору страхування (перестрахування);

2) інформація, що становить таємницю фінансової послуги, яка обробляється в інформаційно-комунікаційних системах надавача фінансових послуг;

3) інформаційно-комунікаційні системи надавача фінансових послуг, що підтримують основні бізнес-процеси надавача фінансових послуг та/або взаємодіють з інформаційними системами Національного банку.

6. Надавач фінансових послуг зобов'язаний:

1) вживати заходів із забезпечення інформаційної безпеки та кіберзахисту на всіх стадіях життєвого циклу інформаційно-комунікаційних систем надавача фінансових послуг;

2) запровадити процес управління кіберризиками та ризиками інформаційної безпеки.

7. Надавач фінансових послуг має право:

1) запровадити процес управління кіберризиками та ризиками інформаційної безпеки в межах своєї системи управління ризиками;

2) самостійно визначати підходи (методики) оцінювання та оброблення кіберризиків та ризиків інформаційної безпеки.

8. Надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтований підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту, визначені в цьому Положенні, з урахуванням особливостей

функціонування інформаційно-комунікаційних систем надавача фінансових послуг.

9. Надавач фінансових послуг має право залучати для виконання заходів із забезпечення інформаційної безпеки та з реагування на інциденти інформаційної безпеки та інциденти кібербезпеки (далі – кіберінциденти) осіб, які мають право надавати такі послуги. Водночас обов'язковими умовами є:

1) наявність у договорі норм про нерозголошення інформації (NDA, англійською мовою "Non-disclosure agreement");

2) такою особою не може бути юридична особа, фізична особа-підприємець, що є резидентами держави-агресора чи держави, що здійснює / здійснювала збройну агресію проти України, або мають кінцевих бенефіціарних власників, які є резидентами держави-агресора або держави, що здійснює / здійснювала збройну агресію проти України, або здійснюють обробку або зберігання даних за допомогою технології хмарних обчислень та центрів обробки даних, що розміщені на території держави-агресора, держави, що здійснює / здійснювала збройну агресію проти України, тимчасово окупованій території України, та/або належать суб'єктам, діяльність яких підпадає під дію Закону України "Про санкції" (далі – Закон про санкції) та стосовно яких прийнято рішення про застосування санкцій в Україні.

10. Надавач фінансових послуг зобов'язаний використовувати програмні, апаратні, програмно-апаратні засоби у складі інформаційно-комунікаційних систем надавача фінансових послуг з урахуванням вимог Закону про санкції, Закону про захист інформації, Закону про забезпечення кібербезпеки, інших законів України.

II. Базові вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту

11. Керівник надавача фінансових послуг:

1) здійснює загальну організацію діяльності з виконання вимог з інформаційної безпеки та кіберзахисту;

2) призначає відповідальну особу за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг, здійснює контроль за його діяльністю або особисто виконує функції відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг;

3) затверджує внутрішні документи з питань забезпечення інформаційної безпеки та кіберзахисту, включаючи політику, положення, стандарти, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі, відповідно до вимог цього Положення;

4) затверджує механізми контролю та заходи з управління кіберризиками та ризиками інформаційної безпеки;

5) організовує підготовку та підвищення кваліфікації відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту.

12. Керівник надавача фінансових послуг призначає відповідальну особу за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту надавача фінансових послуг окремим рішенням.

13. 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 інформаційної безпеки відповідно до вимог цього Положення;

3) організовує регулярну, але не рідше одного разу на рік з моменту останньої проведеної актуалізації актуалізацію переліку / реєстру 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) здійснює контроль за недопущенням встановлення та використання у складі інформаційно-комунікаційних систем програмних і апаратних засобів, не передбачених внутрішніми документами надавача фінансових послуг;

7) погоджує зміну програмних та апаратних засобів інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем надавача фінансових послуг.

14. 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 або в інший спосіб, що забезпечує підтвердження ознайомлення.

15. 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 під час надання послуг здійснює обробку інформації, яка віднесена до таємниці фінансової послуги.

16. Надавач фінансових послуг зобов’язаний забезпечити розподіл прав доступу до інформаційно-комунікаційних систем у спосіб, що дає змогу:

1) визначати права доступу клієнтів, користувачів та привілейованих користувачів до інформаційно-комунікаційних систем надавача фінансових послуг;

2) здійснити опис груп, ролей та розподіл повноважень клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем (шаблони моделей доступу);

3) визначати права на виконання операцій (читання, модифікація, створення, видалення) для клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем надавача фінансових послуг.

17. Надавач фінансових послуг зобов’язаний:

1) 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;

2) забезпечити дотримання принципу надання мінімального рівня повноважень для користувачів та привілейованих користувачів, достатнього для виконання функціональних обов'язків під час надання доступу до інформаційно-комунікаційних систем.

18. Надавач фінансових послуг зобов'язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо управління правами доступу до інформаційно-комунікаційних систем надавача фінансових послуг і повинні містити:

1) вимоги до ідентифікації, автентифікації, авторизації клієнтів, користувачів та привілейованих користувачів;

2) послідовність дій під час управління правами доступу;

3) порядок здійснення заходів контролю доступу;

4) вимоги до протоколювання дій під час управління правами доступу.

19. Надавач фінансових послуг зобов'язаний:

1) запровадити технології та процедури автентифікації, які повинні впроваджуватися на основі внутрішніх документів, що регламентують контроль доступу для забезпечення автентифікації клієнтів, користувачів та привілейованих користувачів під час надання доступу до інформаційно-комунікаційних систем надавача фінансових послуг;

2) організувати та забезпечити доступ клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем надавача фінансових послуг у межах встановлених для них прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) клієнта, користувача, привілейованого користувача і пароля, що вводиться клієнтом, користувачем, привілейованим користувачем, або програмно-апаратного ідентифікатора (ключ, сертифікат, токен, біометрія).

20. Надавач фінансових послуг зобов'язаний запровадити та використовувати багатофакторну (множинну) автентифікацію для користувачів та привілейованих користувачів під час здійснення ними віддаленого доступу до інформаційно-комунікаційних систем надавача фінансових послуг.

Надавач фінансових послуг має право використовувати біометрію лише як один із факторів багатофакторної автентифікації.

21. Надавач фінансових послуг зобов'язаний забезпечити блокування / видалення облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах надавача фінансових послуг:

1) у разі кількох (до п'яти) невдалих спроб автентифікації поспіль (автоматичне тимчасове або постійне блокування);

2) якщо не було 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;

3) у разі звільнення користувача, привілейованого користувача або зміни статусу / функціональних обов'язків користувача, привілейованого користувача, який не передбачає доступу до цих систем;

4) у разі завершення дії договору з клієнтом (крім страховиків) або втрати клієнтом членства в кредитній спілці (для кредитних спілок).

22. Надавач фінансових послуг зобов'язаний визначити та запровадити посилені вимоги до паролів для облікових записів привілейованих користувачів (довжина та складність паролів, частота зміни) або застосовувати багатофакторну автентифікацію для таких облікових записів. Привілейовані користувачі надавача фінансових послуг зобов'язані використовувати різні облікові записи для виконання функцій, які потребують привілейованих прав доступу, та повсякденних завдань.

23. Користувачі зобов'язані використовувати складні паролі, які мають не менше ніж 12 символів та містять цифри, букви в різних регістрах та спеціальні символи (за умов, що система підтримує спеціальні символи). Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менше ніж 15 символів та містять цифри, букви в різних регістрах та спеціальні символи (за умов, що система підтримує спеціальні символи).

24. 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. Повторення вибраного складного пароля може здійснюватися не раніше ніж на восьмий раз.

25. Надавач фінансових послуг зобов'язаний забезпечити:

1) можливість маскування значення пароля під час введення його клієнтом, користувачем та привілейованим користувачем;

2) 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;

3) 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);

4) ідентифікацію обладнання користувачів та привілейованих користувачів (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.

26. Надавач фінансових послуг зобов'язаний забезпечити налаштування інформаційно-комунікаційних систем надавача фінансових послуг у спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події:

1) доступ до інформації з налаштуваннями програмного та апаратного забезпечення систем, журналів реєстрації подій (логи);

2) результати ідентифікації та автентифікації клієнтів, користувачів та привілейованих користувачів;

3) реєстрація подій, пов'язаних з управлінням правами доступу користувачів та привілейованих користувачів до інформаційно-комунікаційних систем та інформації, що циркулює в них;

4) авторизація / закриття сеансу роботи клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах;

5) невдалі спроби ідентифікації, автентифікації, авторизації клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах та перевищення граничної кількості спроб введення пароля;

6) реєстрація, видалення (блокування) облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах;

7) зміна пароля клієнта, користувача та привілейованого користувача в інформаційно-комунікаційних системах;

8) реєстрація подій, пов’язаних зі зміною конфігураційних налаштувань інформаційно-комунікаційних систем.

27. Страховик виконує заходи, зазначені в пункті 26 розділу ІІ цього Положення, з урахуванням вимог, визначених у пункті 27 розділу ІІІ Положення № 204.

28. Надавач фінансових послуг зобов’язаний:

1) проводити періодичне, але не рідше одного разу на рік з моменту останнього проведеного архівування архівування журналів реєстрації подій (логи) та забезпечувати зберігання журналів реєстрації подій не менше одного року з моменту архівації, якщо інше не передбачено законодавством України;

2) забезпечити захист журналів реєстрації подій (логи) та/або засобів ведення реєстрації цих подій від несанкціонованого доступу. Доступ до журналів реєстрації подій (логи) та/або засобів ведення реєстрації цих подій має надаватися тільки відповідальній особі;

3) запровадити заходи забезпечення мережевого захисту, які повинні бути задокументовані у внутрішніх документах надавача фінансових послуг;

4) 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.

29. Надавач фінансових послуг у разі підключення 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) із 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 у разі відмови (збою) функціонування засобів захисту;

3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних систем, які не використовуються, у стан “без призначення IP-адреси”/“відключено” (за наявності технічної можливості реалізації);

4) забезпечення захисту від атак типу “відмова в обслуговуванні” та інших відомих мережевих атак.

30. Надавач фінансових послуг зобов’язаний:

1) забезпечити розміщення в зоні мережі з підвищеним рівнем безпеки інформаційно-комунікаційних систем надавача фінансових послуг, серверів та обладнання, що забезпечує функціонування сервісів (надання послуг), які відкриті для доступу клієнтів із зовнішніх мереж;

2) використовувати засоби захисту від шкідливого програмного коду з актуальними базами сигнатур.

31. Надавач фінансових послуг зобов’язаний використовувати операційні системи, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника 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.

32. Надавач фінансових послуг зобов’язаний забезпечити блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів.

33. Надавач фінансових послуг зобов’язаний:

1) використовувати офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника, та/або програмне забезпечення,

розроблене для надавача фінансових послуг відповідно до укладених договорів постачання програмного забезпечення або розроблене самостійно таким надавачем;

2) здійснювати або організовувати здійснення підтримки прикладного програмного забезпечення, розробленого самостійно надавачем фінансових послуг або розробленого для надавача фінансових послуг відповідно до укладених договорів постачання програмного забезпечення, включаючи оновлення безпеки, якщо інше не передбачено договором постачання програмного забезпечення.

34. Надавач фінансових послуг зобов'язаний провести аналіз ризиків, пов'язаних з використанням програмного забезпечення, для якого припинено підтримку виробника / розробника або постачальника, та впровадити додаткові компенсуючі заходи, що включають:

1) упровадження додаткових заходів безпеки для захисту інформації (даних) та інформаційно-комунікаційних систем надавача фінансових послуг від потенційних загроз;

2) регулярний моніторинг та аудит інформаційної безпеки для виявлення та усунення вразливостей;

3) забезпечення резервного копіювання інформації (даних) та реалізації плану реагування на кіберінциденти та інциденти інформаційної безпеки з метою відновлення діяльності надавача фінансових послуг у разі настання таких інцидентів;

4) документування та затвердження результатів аналізу ризиків відповідно до внутрішніх документів з питань забезпечення інформаційної безпеки та кіберзахисту;

5) розробку плану переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника.

35. Надавач фінансових послуг зобов'язаний реалізувати заходи, визначені планом переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника в строк, що не перевищує двох років, якщо інше не передбачено законом.

36. План переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від

виробника / розробника або постачальника затверджується наглядовою радою надавача фінансових послуг або іншим органом управління такої особи, відповідальним за здійснення нагляду за її діяльністю, та є складовою стратегії та/або плану діяльності, та/або плану безперервної діяльності надавача фінансових послуг, та/або іншого внутрішнього документа.

37. Надавач фінансових послуг зобов’язаний розробити та затвердити внутрішні документи, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і повинні містити положення щодо:

1) контролю за використанням змінних носіїв інформації, включаючи процедури їх обліку та виведення з експлуатації;

2) категорії інформації, яка може оброблятися на змінних носіях інформації;

3) обов’язкової ідентифікації змінних носіїв інформації, які використовуються надавачем фінансових послуг за допомогою унікального ідентифікатора, який дає змогу визначити тип носія та користувача змінного носія;

4) обмежень використання змінних носіїв інформації;

5) знищення інформації на змінних носіях інформації перед їх передаванням у користування іншому працівникові надавача фінансових послуг, третім особам або виведенням з експлуатації;

6) обов’язкової перевірки змінних носіїв інформації на наявність шкідливого програмного забезпечення перед використанням надавачем фінансових послуг.

38. Надавач фінансових послуг зобов’язаний здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дасть змогу визначити тип носія та користувача змінного носія.

ІІІ. Управління кіберінцидентами та інцидентами інформаційної безпеки

39. Надавач фінансових послуг для забезпечення ефективного реагування на кіберінциденти та інциденти інформаційної безпеки зобов’язаний упровадити процес управління кіберінцидентами та інцидентами інформаційної безпеки, розробити і затвердити план реагування на кіберінциденти та інциденти інформаційної безпеки.

40. Планування реагування на кіберінциденти та інциденти інформаційної безпеки є частиною планування на випадок надзвичайних ситуацій для надавача фінансових послуг і має розглядатися в сукупності із реагуванням на інші інциденти безпеки. План реагування на кіберінциденти та інциденти інформаційної безпеки повинен бути розроблений з урахуванням внутрішніх документів з питань забезпечення безперервності діяльності або бути складовою плану безперервної діяльності надавача фінансових послуг.

41. План реагування на кіберінциденти та інциденти інформаційної безпеки повинен містити:

1) оцінки негативного впливу (збитку), нанесеного надавачу фінансових послуг кіберінцидентом та інцидентом інформаційної безпеки;

2) порядок дій відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту під час реагування на кіберінциденти та інциденти інформаційної безпеки;

3) описи дій користувачів та привілейованих користувачів у разі впровадження кіберінцидентів та інцидентів інформаційної безпеки;

4) порядок взаємодії відповідальної особи за забезпечення виконання вимог з інформаційної безпеки та кіберзахисту з працівниками основних бізнес-процесів надавача фінансових послуг під час реагування на кіберінциденти та інциденти інформаційної безпеки;

5) порядок інформування керівника надавача фінансових послуг про кіберінциденти та інциденти інформаційної безпеки;

6) описи дій зі зберігання інформації щодо кіберінцидентів та інцидентів інформаційної безпеки, їх аналізу та результатів реагування.

42. Надавач фінансових послуг з метою оперативного реагування на кіберінциденти та забезпечення безперервності надання основних послуг зобов’язаний забезпечити взаємодію з особами, зазначеними в пункті 9 розділу I цього Положення, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем.

43. Надавач фінансових послуг зобов’язаний в договорі з особами, зазначеними в пункті 9 розділу I цього Положення, передбачити умови, згідно з якими така особа взаємодіятиме з надавачем фінансових послуг із питань реагування на кіберінциденти та інциденти інформаційної безпеки. Надавач фінансових послуг зобов’язаний під час дії цього договору здійснювати

моніторинг подій, зокрема кіберінцидентів, інцидентів інформаційної безпеки, інцидентів порушення безперервності діяльності, що впливають (можуть вплинути) на надання послуг.

44. Національний банк має право вимагати від надавача фінансових послуг надання інформації щодо реагування на кіберінциденти та інциденти інформаційної безпеки шляхом надсилання письмової вимоги.

45. Письмова вимога оформляється в електронній формі у вигляді листа Національного банку та надсилається засобами системи електронної пошти Національного банку.

46. Керівник надавача фінансових послуг зобов’язаний забезпечити надання на письмову вимогу Національного банку достовірної інформації у вигляді письмових пояснень, документів в електронній або паперовій формі, у спосіб, строк, в обсязі, за форматом та структурою, визначеними в такій письмовій вимозі.