Офіційно опубліковано 28.05.2021

Правління Національного банку України

П О С Т А Н О В А

19 травня 2021 року м. Київ № 43

Про затвердження Положення про захист інформації
та кіберзахист у платіжних системах

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 14, 17, 18, 19, 22, 38 Закону України “Про платіжні системи та переказ коштів в Україні”, статей 6, 8 Закону України “Про основні засади забезпечення кібербезпеки України”, з метою встановлення вимог щодо забезпечення захисту інформації та кіберзахисту в платіжних системах Правління Національного банку України **постановляє:**

1. Затвердити Положення про захист інформації та кіберзахист у платіжних системах (далі – Положення), що додається.

2. Платіжним організаціям платіжних систем, учасникам/членам платіжних систем та операторам послуг платіжної інфраструктури протягом 12 місяців із дня набрання чинності цією постановою:

1) розробити/доопрацювати з урахуванням вимог Положення та затвердити внутрішні документи щодо інформаційної безпеки та кіберзахисту;

2) привести свою діяльність у відповідність до вимог Положення.

3. Департаменту безпеки (Ігор Коновалов) після офіційного опублікування довести до відома платіжних організацій платіжних систем, учасників/членів платіжних систем, операторів послуг платіжної інфраструктури інформацію про прийняття цієї постанови.

4. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Кирила Шевченка.

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

Голова Кирило ШЕВЧЕНКО

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
19 травня 2021 року № 43

Положення
про захист інформації та кіберзахист у платіжних системах

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про платіжні системи та переказ коштів в Україні”, “Про основні засади забезпечення кібербезпеки України”, “Про електронні довірчі послуги”.

2. Це Положення визначає вимоги та заходи щодо забезпечення захисту інформації, кіберзахисту та інформаційної безпеки у сфері переказу коштів та контроль за їх виконанням.

3. Терміни, що використовуються в цьому Положенні, вживаються в такому значенні:

1) адміністратор – призначена керівником, його заступником або керівним органом суб’єкта інформаційного захисту (далі – керівництво) відповідальна особа, яка забезпечує супровід та управління програмними та/або апаратними засобами чи ресурсами;

2) багатофакторна автентифікація – автентифікація із використанням двох (або більше) різних типів електронних ідентифікаційних даних;

3) віртуальна машина – емуляція комп’ютерної системи, яка забезпечує функціональність фізичного комп’ютера та працює під управлінням гіпервізора;

4) гіпервізор – сукупність програмних та апаратних засобів, що забезпечують паралельне функціонування кількох віртуальних машин на одному комп’ютері, ізолюючи ці віртуальні машини та можливість керування наявними ресурсами, можливість розподілення ресурсів між віртуальними машинами, що використовуються;

5) засіб захисту мережі – програмний або апаратний засіб, який захищає інформаційну систему, що використовується для переказу коштів (далі – ІС), від несанкціонованого доступу до її мережевих складових, випадкового або навмисного втручання в роботу мережі;

6) інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації;

7) інцидент інформаційної безпеки – подія або серія подій порушення інформаційної безпеки, які можуть призвести до збитків та втрат для суб'єкта інформаційного захисту або користувачів платіжних систем;

8) керівник суб'єкта інформаційного захисту – призначена власником суб'єкта інформаційного захисту посадова особа, яка діє від імені суб'єкта інформаційного захисту, представляє його інтереси в органах державної влади і органах місцевого самоврядування, інших організаціях, у відносинах з юридичними особами та громадянами, формує адміністрацію суб'єкта інформаційного захисту і вирішує питання діяльності суб'єкта інформаційного захисту в межах та порядку, визначених установчими документами;

9) кіберінцидент – подія або сукупність несприятливих подій ненавмисного характеру або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці інформаційної інфраструктури, створюють імовірність порушення штатного режиму її функціонування, а також ставлять під загрозу захищеність інформаційних ресурсів;

10) ключовий суб'єкт інформаційного захисту – суб'єкт інформаційного захисту, який належить до однієї категорії або більше:

платіжна організація значущої платіжної системи, якщо вона виконує функції оператора послуг платіжної інфраструктури в цій платіжній системі;

значущий оператор послуг платіжної інфраструктури;

оператор послуг платіжної інфраструктури, який обслуговує платіжну систему, створену нерезидентом, та яка отримала дозвіл Національного банку України (далі – Національний банк) надавати свої послуги в Україні;

оператор послуг платіжної інфраструктури, який обслуговує більше ніж одну платіжну систему;

11) користувач ІС – уповноважений працівник суб'єкта інформаційного захисту, що має можливість здійснювати створення, перегляд, оброблення, модифікацію, збереження та видалення інформації в ІС;

12) криптографічний алгоритм – алгоритм, який визначає правила перетворення інформації з метою її криптографічного захисту;

13) критичне приміщення – центр оброблення даних, серверна кімната або інше приміщення, в якому розміщені системи, які здійснюють оброблення, зберігання або передавання електронних документів на переказ, архівів та/або інших критичних даних;

14) критичні дані – дані, несанкціоноване використання яких призводить до порушення інформаційної безпеки або порушення прав користувачів платіжної системи;

15) несанкціонований доступ (далі – НСД) – отримання доступу до комп'ютерної системи або вчинення дій, які призводять до одержання доступу до інформації особою, яка не має прав на перегляд та/або модифікацію цієї інформації без дозволу керівництва або уповноважених ним осіб;

16) суб'єкт інформаційного захисту – платіжна організація платіжної системи, створеної в Україні резидентом України, учасник платіжної системи (резидент/нерезидент), який надає послуги з переказу коштів в Україні на законних підставах (далі – учасник платіжної системи), оператор послуг платіжної інфраструктури (у разі надання інших видів послуг, крім оброблення інформації за операціями в міжнародних карткових платіжних системах).

Інші терміни в цьому Положенні вживаються в значеннях, наведених у законах України та нормативно-правових актах Національного банку.

4. Вимоги цього Положення поширюються на суб'єктів інформаційного захисту, крім учасників міжнародних платіжних систем, створених нерезидентами, що на законних підставах надають послуги в Україні та використовують засоби захисту інформації відповідно до правил цих платіжних систем та з урахуванням вимог юрисдикцій, де їхні правила були узгоджені, на банки, що є платіжними організаціями та/або учасниками платіжних систем, створених резидентами, у частині питань, що не врегульовані іншими нормативно-правовими актами Національного банку у сфері кіберзахисту та інформаційної безпеки в банківській системі.

5. Вимоги цього Положення не поширюються на платіжні системи, створені Національним банком.

6. Вимоги цього Положення поширюються на:

1) електронні документи на переказ;

2) інформаційні повідомлення між суб'єктами інформаційного захисту, пов'язані з переказом коштів;

3) бази даних, що містять інформацію, пов’язану з переказом коштів;

4) сервери та мережеве обладнання, що використовуються для переказу коштів;

5) засоби захисту інформації (технічні та криптографічні);

6) криптографічні ключі.

7. Контроль за виконанням вимог цього Положення здійснює Національний банк.

ІІ. Вимоги до організаційного забезпечення діяльності з питань захисту інформації та кіберзахисту

8. Суб’єкт інформаційного захисту забезпечує виконання вимог цього Положення щодо програмних, апаратних засобів і комплексів, мережевого обладнання, які ним використовуються для переказу коштів, а також щодо документів, передбачених цим Положенням.

9. Керівник суб’єкта інформаційного захисту здійснює загальну організацію діяльності з питань забезпечення захисту інформації, кіберзахисту та інформаційної безпеки.

Керівник суб’єкта інформаційного захисту з цією метою:

1) призначає відповідальних осіб за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки і здійснює контроль за їхньою діяльністю;

2) затверджує політику інформаційної безпеки та документи, зазначені в пунктах 11, 13 розділу ІІІ цього Положення.

10. Відповідальні особи за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки суб’єкта інформаційного захисту:

1) організовують виконання вимог цього Положення;

2) здійснюють контроль за виконанням заходів щодо забезпечення кіберзахисту та інформаційної безпеки на всіх стадіях життєвого циклу (проєктування, впровадження, експлуатації та виведення з експлуатації) ІС суб’єкта інформаційного захисту;

3) розробляють політику інформаційної безпеки та документи, зазначені в пунктах 11, 13 розділу ІІІ цього Положення;

4) здійснюють моніторинг та розслідування інцидентів інформаційної безпеки та кіберінцидентів, які стосуються переказу коштів;

5) організовують контроль за працездатністю засобів захисту інформації та відновлення їх працездатності в разі порушення функціонування;

6) здійснюють контроль за складом і цілісністю програмних та апаратних засобів ІС, уживають заходів щодо недопущення встановлення та використання в складі ІС програмних і апаратних засобів, не передбачених документами з питань захисту інформації, кіберзахисту та інформаційної безпеки;

7) погоджують зміну програмних та апаратних засобів ІС з урахуванням вимог законодавства України та правил платіжних систем щодо захисту інформації, кіберзахисту та інформаційної безпеки;

8) організовують підготовку та підвищення кваліфікації фахівців, які беруть участь у реалізації заходів щодо захисту інформації, кіберзахисту та інформаційної безпеки.

ІІІ. Вимоги до нормативного забезпечення діяльності з питань захисту інформації, кіберзахисту та інформаційної безпеки

11. Суб’єкт інформаційного захисту повинен до початку своєї діяльності розробити такі внутрішні документи з питань захисту інформації, кіберзахисту та інформаційної безпеки в платіжних системах:

1) політику інформаційної безпеки, що включає мету, завдання та загальні принципи забезпечення захисту інформації, кіберзахисту та інформаційної безпеки, перелік об’єктів, що підлягають захисту, моделі загроз та моделі порушників, основні положення щодо забезпечення захисту інформації, кіберзахисту та інформаційної безпеки, відповідальність за дотримання положень політики та контроль за її дотриманням;

2) документи, що визначають повноваження та відповідальність персоналу з питань забезпечення захисту інформації, кіберзахисту та інформаційної безпеки;

3) вимоги щодо захисту особистих ключів підписувачів від НСД;

4) методику відновлення та захисту критичних даних у разі втрати, компрометації чи пошкодження криптографічних ключів або носіїв критичних даних.

До критичних даних належать:

електронні документи на переказ;

паролі;
персональні дані;
архіви всіх цих даних;

5) вимоги до паролів, що не суперечать вимогам, визначеним у пункті 12 розділу ІІІ цього Положення.

12. Паролі, які використовує суб'єкт інформаційного захисту, повинні відповідати таким вимогам:

1) паролі користувачів платіжних систем та користувачів ІС створюються під час реєстрації;

2) зберігання та передавання паролів здійснюється в захищеному від НСД вигляді;

3) пароль дійсний для одноразового використання не більше 10 хвилин та може передаватися через мережі загального користування (електронна пошта, електронні повідомлення) у разі використання як одного з факторів багатофакторної автентифікації;

4) паролі доступу повинні мати довжину не менше восьми символів, серед яких повинні використовуватися малі та великі латинські літери (принаймні одна велика і одна мала літера), арабські цифри (принаймні одна) та спеціальні символи (принаймні один);

5) паролі відповідальних осіб за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки повинні змінюватися не рідше ніж один раз на 120 діб;

6) паролі доступу до облікових записів для адміністрування гіпервізорів та серверів повинні змінюватися не рідше ніж один раз на 90 діб.

13. Ключовий суб'єкт інформаційного захисту зобов'язаний розробити додатково до передбачених у пункті 11 розділу ІІІ цього Положення такі внутрішні документи з питань захисту інформації, кіберзахисту та інформаційної безпеки в платіжних системах:

1) політику резервного копіювання, яка повинна містити порядок виконання процедур резервного копіювання електронних документів на переказ, регламент перевірки цілісності та працездатності резервних копій;

2) політику обмеження використання змінних носіїв інформації;

3) політику захисту від шкідливого програмного забезпечення (далі – ПЗ), зловмисного коду та вірусів.

14. Внутрішні документи, зазначені в пунктах 11, 13 розділу ІІІ цього Положення, можуть бути одним документом. Внутрішні документи з питань захисту інформації, кіберзахисту та інформаційної безпеки переглядаються за потреби, але не рідше ніж один раз на два роки, а також у зв'язку зі змінами в законодавстві України або нормативно-правових актах Національного банку.

IV. Управління системою захисту

15. Суб'єкт інформаційного захисту зобов'язаний вживати заходів для забезпечення захисту інформації, кіберзахисту та інформаційної безпеки на всіх стадіях життєвого циклу системи захисту, що використовується для переказу коштів: під час підготовки до експлуатації, під час уведення в експлуатацію, під час експлуатації і під час зняття з експлуатації.

16. Суб'єкт інформаційного захисту під час формування вимог до системи захисту повинен враховувати вимоги до захисту інформації та кіберзахисту законодавства України та цього Положення.

Суб'єкт інформаційного захисту зобов'язаний формувати вимоги до системи захисту інформації за результатами:

1) виявлення джерел загроз інформаційній безпеці та кібербезпеці, оцінювання можливостей потенційних зовнішніх і внутрішніх порушників;

2) аналізу можливих уразливостей всіх складових ІС;

3) оцінювання можливих наслідків від виникнення загроз інформаційній безпеці та порушення властивостей системи захисту інформації в цілому.

17. Ключовий суб'єкт інформаційного захисту повинен:

1) забезпечувати безперервну технічну підтримку системи захисту інформації, що ним використовується;

2) проводити функціональні випробування новоствореного чи доопрацьованого ключовим суб'єктом інформаційного захисту ПЗ, що забезпечує захист інформації, перед його впровадженням у дослідну чи промислову експлуатацію;

3) під час розроблення, впровадження та експлуатації власного ПЗ, що використовується для захисту інформації, забезпечувати усунення всіх відомих вразливостей, що впливають на досягнення мети розроблення.

V. Фізичний захист

18. Суб’єкт інформаційного захисту зобов’язаний забезпечити розміщення серверів, що використовуються для зберігання та оброблення електронних документів на переказ, персональних даних користувачів платіжних систем та архівів цих даних, у критичних приміщеннях. Перелік працівників суб’єкта інформаційного захисту, яким надається право постійного доступу до цих серверів, визначається відповідальною особою та затверджується керівником суб’єкта або його заступником. Доступ інших осіб до цих серверів надається за погодженням із відповідальною особою та в супроводі працівників, які мають право постійного доступу до цих серверів.

Суб’єкт інформаційного захисту в разі використання серверного та мережевого обладнання на умовах оренди визначає порядок доступу до цього обладнання на договірних засадах з урахуванням вимог цього Положення.

19. Критичні приміщення мають відповідати таким вимогам:

1) обладнані технічними засобами охорони та засобами відеоспостереження для моніторингу відвідувань;

2) не містять обладнаних постійних робочих місць;

3) використовуються резервні джерела живлення для захисту серверного та мережевого обладнання, що здатні забезпечувати постачання електроенергії на період, необхідний для зберігання результатів роботи та здійснення штатного вимкнення всього обладнання;

4) мережева інфраструктура, яка міститься в критичних приміщеннях, не використовує безпровідні технології;

5) фіксуються дії щодо встановлення, видалення чи заміни носіїв інформації на серверах.

VI. Ідентифікація та автентифікація

20. Суб’єкту інформаційного захисту забороняється під час промислової експлуатації програмних та апаратних засобів здійснювати будь-яку ідентифікацію та автентифікацію з використанням даних, установлених за замовчуванням виробником обладнання.

21. Суб’єкт інформаційного захисту повинен забезпечити виконання таких вимог під час автентифікації користувачів платіжних систем та користувачів ІС у разі віддаленого підключення до таких ІС:

1) пароль, що використовується для автентифікації, не повинен передаватися через незахищені мережі та зберігатися в базах даних у відкритому вигляді;

2) повинна застосовуватися багатофакторна автентифікація;

3) заборонено використовувати для автентифікації соціальні мережі та інші вебсервіси загального користування.

VII. Управління доступом

22. Суб'єкт інформаційного захисту зобов'язаний забезпечити розроблення, документування, узгодження з платіжною організацією платіжної системи та періодичне оновлення політики управління доступом у платіжній системі, а також заходів, пов'язаних із реалізацією цієї політики.

23. Політика управління доступом повинна визначати:

1) порядок створення, активації, модифікації, перегляду, блокування, відключення, видалення, контролю за використанням облікових записів користувачів ІС, типи облікових записів залежно від їхньої категорії;

2) методи управління доступом, типи доступу користувачів ІС до засобів захисту мережі та програмно-апаратних комплексів, які підлягають захисту;

3) правила розмежування доступу користувачів ІС.

24. Суб'єкт інформаційного захисту зобов'язаний забезпечити захист інформації щодо переказу коштів, що передається в його внутрішній мережі, від НСД шляхом виконання таких вимог:

1) доступ користувачів платіжних систем та доступ користувачів ІС у разі віддаленого підключення до цих систем повинен здійснюватися через єдину точку мережевого входу з використанням засобу захисту мережі;

2) засіб захисту мережі повинен контролювати та фільтрувати IP-адреси і порти віддалених з'єднань та IP-адреси у внутрішній мережі;

3) віддалені з'єднання із засобом захисту мережі повинні протоколюватися;

4) доступ до внутрішніх IP-адрес із мереж загального користування повинен бути неможливим;

5) сервери, що забезпечують функціонування сервісів, відкритих для доступу з мереж загального користування, повинні розміщуватися в демілітаризованій зоні;

6) обмеження доступу між демілітаризованою зоною та іншими сегментами мережі повинно здійснюватися з використанням засобів захисту мережі;

7) шифрування каналу обміну інформацією між серверами, розміщеними в різних критичних приміщеннях та об'єднаними за допомогою мереж загального користування, повинно забезпечуватися з використанням захищених від НСД криптографічних ключів;

8) повинен забезпечуватися захист від НСД облікових даних та паролів доступу до серверів і мережевого обладнання.

VIII. Захист від шкідливого ПЗ, зловмисного коду та вірусів

25. Суб'єкт інформаційного захисту зобов'язаний забезпечити захист ІС від шкідливого ПЗ, зловмисного коду та вірусів шляхом:

1) використання спеціалізованих засобів захисту від зловмисного коду, шкідливого ПЗ та вірусів, їх своєчасного оновлення;

2) визначення переліку ПЗ та переліку складових цього ПЗ, дозволених до використання в ІС;

3) використання на серверах лише тих системних утиліт, які необхідні для функціонування серверного ПЗ;

4) своєчасного встановлення пакетів оновлень ПЗ, що випускаються розробниками ПЗ;

5) обмеження переліку складових ПЗ, що запускаються автоматично під час завантаження операційних систем;

6) моніторингу та ведення обліку спроб несанкціонованої зміни ПЗ та блокування таких спроб.

26. Суб'єкт інформаційного захисту зобов'язаний попередити своїх працівників про неприпустимість використання шкідливого ПЗ та ПЗ із порушенням авторського права.

IX. Забезпечення мережевого захисту

27. Адміністратор засобів захисту мережі суб’єкта інформаційного захисту здійснює адміністрування одним із таких способів:

1) шляхом безпосереднього фізичного доступу до консолі пристрою;

2) через захищений від НСД канал доступу з робочого місця адміністратора.

28. Суб’єкт інформаційного захисту під час експлуатації засобу захисту мережі повинен:

1) забезпечити відключення всіх сервісів, які не є необхідними для експлуатації засобу захисту мережі;

2) забезпечити можливість скасування змін, унесених до системи конфігурації засобу захисту мережі, та відновлення попередньої версії внутрішнього ПЗ;

3) розміщувати засіб захисту мережі, реалізований програмними засобами, на окремому сервері (фізичному або віртуальному).

29. Ключовий суб’єкт інформаційного захисту під час експлуатації засобу захисту мережі зобов’язаний забезпечити своєчасне встановлення актуальних оновлень ПЗ засобу захисту мережі від виробника.

30. Суб’єкт інформаційного захисту в разі створення віртуальної приватної мережі для обміну критичними даними повинен використовувати лише ті криптографічні алгоритми шифрування, які є національними стандартами, або ті, на які за результатами державної експертизи Державної служби спеціального зв’язку та захисту інформації України (далі – Адміністрація Держспецзв’язку) видано позитивний експертний висновок.

X. Вимоги до використання ІС

31. Доступ користувачів до складових ІС, що перебувають у внутрішній мережі, допускається лише через засіб захисту мережі.

32. Суб’єкту інформаційного захисту під час проєктування та використання своїх ІС забороняється використання ПЗ та технічних пристроїв, розробником та/або виробником яких є юридична чи фізична особа, стосовно якої діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України.

33. Суб’єкт інформаційного захисту зобов’язаний забезпечити блокування облікового запису адміністратора чи користувача ІС у разі більше п’яти невдалих спроб автентифікації поспіль (автоматичне блокування).

XI. Вимоги до криптографічних засобів захисту інформації та середовища віртуалізації

34. Суб’єкт інформаційного захисту зобов’язаний застосовувати засоби криптографічного захисту інформації, що мають діючий сертифікат відповідності або виданий за результатами державної експертизи Адміністрацією Держспецзв’язку позитивний експертний висновок, у разі:

1) створення та перевірки електронних підписів;

2) шифрування криптографічних ключів, а також інформаційних повідомлень між суб’єктами інформаційного захисту, пов’язаними з переказом коштів, під час їх передавання через мережі загального користування;

3) підтвердження цілісності, достовірності та авторства даних на електронних носіях, що містять архіви електронних документів.

35. Суб’єкт інформаційного захисту має право використовувати для переказу коштів віртуальні сервери під управлінням гіпервізора з обов’язковим дотриманням таких вимог:

1) повинні реєструватися всі дії адміністраторів віртуальних серверів та гіпервізора;

2) повинен здійснюватися контроль за цілісністю налаштувань гіпервізора;

3) оновлення ПЗ гіпервізора повинно виконуватися виключно адміністратором гіпервізора;

4) гіпервізор, на якому працює одна чи кілька віртуальних машин, повинен бути захищеним від зовнішнього НСД за допомогою окремого засобу захисту мережі;

5) файли образів віртуальних машин повинні зберігатися в нешифрованому вигляді лише в критичних приміщеннях, а їх передавання повинно здійснюватися виключно із забезпеченням конфіденційності та цілісності;

6) дані гіпервізора, необхідні для відновлення його працездатності, повинні зберігатися.

XII. Умови використання електронного підпису

36. Учасник міжнародної платіжної системи, створеної нерезидентом, або оператор послуг платіжної інфраструктури, який забезпечує взаємодію з міжнародною платіжною системою, платіжною організацією якої є нерезидент, повинен укласти договір із платіжною організацією такої платіжної системи про визнання електронного підпису.

37. Суб'єкт інформаційного захисту (учасник міжнародної платіжної системи, створеної нерезидентом, або оператор послуг платіжної інфраструктури), якщо немає визнаного електронного підпису на електронному документі на переказ, який отримано від платіжної організації міжнародної платіжної системи, створеної нерезидентом, зобов'язаний накласти свій електронний підпис на цей електронний документ відповідно до законодавства України.

38. Суб'єкт інформаційного захисту має право використовувати вдосконалений електронний підпис без сертифіката відкритого ключа або чинність відкритого ключа підписувача засвідчується сертифікатом відкритого ключа на договірних засадах.

XIII. Вимоги щодо фіксації кіберінцидентів та інцидентів інформаційної безпеки і реагування на них

39. Суб'єкт інформаційного захисту зобов'язаний забезпечити розроблення, документування, узгодження з платіжною організацією платіжної системи та періодичне оновлення політики управління інцидентами в платіжній системі, а також заходів, пов'язаних із реалізацією цієї політики.

40. Політика управління інцидентами повинна містити:

1) перелік та класифікацію подій, що належать до порушення вимог інформаційної безпеки, інцидентів інформаційної безпеки та кіберінцидентів (далі – події);

2) процедури виявлення та реєстрації подій, збору інформації про події;

3) порядок реагування на події в разі їх виникнення;

4) порядок складання звітів та інформування про події;

5) ролі та відповідальність працівників і адміністраторів за реалізацію політики управління інцидентами.

41. Мінімальні вимоги до ІС суб’єкта інформаційного захисту передбачають, що ІС повинна забезпечувати автоматичну реєстрацію таких подій:

1) результатів ідентифікації та автентифікації користувачів ІС (вдалі та невдалі спроби);

2) фактів створення, видалення, блокування облікових записів користувачів ІС;

3) фактів надання та позбавлення користувачів ІС права доступу до інформації;

4) результатів виконання користувачем ІС операцій з оброблення інформації та спроб несанкціонованої модифікації інформації.

42. Засоби реєстрації подій повинні фіксувати інформацію про дату, час, місце, тип, успішність чи неуспішність кожної зареєстрованої події. Записи про події інформаційної безпеки повинні містити достатньо інформації для визначення події, що сталася, її джерела.

43. Відповідальні особи за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки повинні регулярно переглядати і аналізувати зареєстровані події з метою виявлення незвичайної або підозрілої активності, складати звіти і діяти відповідно до документів суб’єкта інформаційного захисту.

44. Засоби реєстрації подій та записи про зареєстровані події мають бути захищеними від модифікації та знищення користувачами ІС, які не мають повноважень адміністратора.

45. Суб’єкт інформаційного захисту зобов’язаний невідкладно повідомити Національний банк, якщо виявлено:

1) події, що містять ознаки злочинів, передбачених у розділі XVI Кримінального кодексу України;

2) події, які класифікуються згідно із Законом України “Про основні засади забезпечення кібербезпеки України” як кіберінциденти;

3) події, що призвели до витоку чи незаконного розголошення інформації з обмеженим доступом, яка обробляється в ІС.

46. Повідомлення про події, зазначені в пункті 45 розділу XIII цього Положення, слід надавати одним із таких способів:

1) електронним листом засобами системи електронної пошти Національного банку;

2) електронним листом на офіційну електронну поштову скриньку Національного банку;

3) засобами поштового зв’язку на паперовому носії (у разі неможливості використання вищезазначених засобів електронного зв’язку).