ПРОЕКТ

Правління Національного банку України

П О С Т А Н О В А

м. Київ №

Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 6, 8 Закону України “Про основні засади забезпечення кібербезпеки України”, з метою встановлення вимог із забезпечення кіберзахисту та інформаційної безпеки для суб’єктів переказу коштів Правління Національного банку України **постановляє:**

1. Затвердити Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків (далі – Положення), що додається.

2. Платіжним організаціям платіжних систем, учасникам/членам платіжних систем та операторам послуг платіжної інфраструктури до 01 липня 2019 року:

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 (Скомаровський О. А.) 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 Смолія Я. В.

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

Голова Я. В. Смолій

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Положення
про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про платіжні системи та переказ коштів в Україні", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні документи та електронний документообіг", "Про основні засади забезпечення кібербезпеки України", "Про електронні довірчі послуги", Указу Президента України від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

2. Це Положення визначає обов'язкові мінімальні вимоги до забезпечення інформаційної безпеки та кіберзахисту в сфері переказу коштів.

3. Дія цього Положення поширюється на:

1) платіжні організації платіжних систем та систем розрахунків, створених резидентами України;

2) учасників-резидентів платіжних систем та систем розрахунків, створених як резидентами, так і нерезидентами України;

3) операторів послуг платіжної інфраструктури;

4) платіжні організації міжнародних платіжних систем, створених нерезидентами, у частині їх діяльності на території України (далі – суб'єкти платіжного ринку).

4. Дія цього Положення не поширюється на платіжні системи, створені Національним банком України (далі – Національний банк).

5. Терміни, що використовуються у цьому Положенні, вживаються в таких значеннях:

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

2) адміністратор – призначена керівником, його заступником або керівним органом суб'єкта платіжного ринку відповідальна особа, яка забезпечує процеси супроводу та управління програмними та/або апаратними засобами чи ресурсами;

3) віртуальна машина – екземпляр обчислювального середовища, що працює під управлінням гіпервізора;

4) гіпервізор – комп'ютерна програма або апаратна схема, що забезпечує одночасне, паралельне виконання кількох операційних систем на одному комп'ютері, забезпечуючи ізоляцію операційних систем, розділення ресурсів між працюючими операційними системами і керування ресурсами;

5) демілітаризована зона – сегмент комп'ютерної мережі, у якому розміщуються сервери, що відповідають на запити із зовнішньої мережі, і доступ до якого з інших сегментів мережі обмежено за допомогою засобів мережевого екранування з метою мінімізації потенційних ризиків кібератак та інцидентів кібербезпеки;

6) засоби мережевого екранування – пристрій або сукупність пристроїв, що дають змогу налаштувати обмеження передавання даних між зонами з різним рівнем безпеки відповідно до заданих набором правил чи критеріїв;

7) ключовий суб'єкт платіжного ринку – суб'єкт платіжного ринку, який є:
або платіжною організацією значущої платіжної системи, якщо вона виконує функції оператора послуг платіжної інфраструктури,
або значущим оператором послуг платіжної інфраструктури,
або оператором послуг платіжної інфраструктури, який обслуговує платіжну систему, створену нерезидентом,
або оператором послуг платіжної інфраструктури, який обслуговує більш ніж одну платіжну систему;

8) компонент – програмно-апаратний комплекс суб'єкта платіжного ринку, що розміщений в одному приміщенні та взаємодіє з іншими програмно-апаратними комплексами за допомогою комп'ютерної мережі або є автономним;

9) контрольована зона – зона (територія, будівля, частина будівлі, приміщення), у якій не допускається несанкціоноване перебування працівників та інших осіб;

10) криптографічний алгоритм – набір математичних правил та процедур, за допомогою яких здійснюється криптографічне перетворення інформації;

11) критичне приміщення – центр обробки 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;

12) критичні дані – дані, несанкціоноване використання яких призводить до порушення безпеки інформації в системі або порушення прав користувачів системи;

13) надійні засоби – криптографічні засоби захисту інформації, що мають чинний сертифікат відповідності або позитивний експертний висновок за результатами експертизи у сфері криптографічного захисту інформації одного з таких органів: Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ), Національного інституту стандартів та технології Сполучених Штатів Америки (далі – NIST), Європейського комітету зі стандартизації (далі – CEN);

14) несанкціоноване втручання – проникнення до програмно-апаратних комплексів, автоматизованих систем чи комп'ютерних мереж і вчинення дій, які змінюють або повністю чи частково припиняють режим їх роботи, без згоди (дозволу) керівника чи уповноважених ним осіб;

15) тестування на проникнення – метод оцінювання захищеності комп'ютерних систем або мережі шляхом часткового моделювання дій зовнішніх чи внутрішніх зловмисників із проникненням у систему, що включає в себе активний аналіз системи з виявлення будь-якої потенційної вразливості;

16) твердотільний накопичувач – комп'ютерний запам'ятовуючий пристрій, що не містить рухомих механічних частин.

6. Інші терміни у цьому Положенні вживаються в значеннях, наведених у Законах України "Про основні засади забезпечення кібербезпеки України", "Про електронні довірчі послуги", "Про платіжні системи та переказ коштів в Україні", "Про захист інформації в інформаційно-телекомунікаційних системах", Положенні про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні, затвердженому постановою Правління Національного

банку України від 28 листопада 2014 року № 755 (зі змінами), інших законах України та нормативно-правових актах Національного банку.

7. Національний банк здійснює контроль за дотриманням суб'єктами платіжного ринку вимог цього Положення та законодавства України щодо інформаційної безпеки та кіберзахисту у сфері переказу коштів.

ІІ. Загальні вимоги до суб'єктів платіжного ринку

8. Суб'єкт платіжного ринку забезпечує виконання вимог цього Положення в межах, що відповідають функціональній ролі, яку він здійснює, а також відповідно до програмних, апаратних засобів і комплексів, мережевого обладнання, які ним використовуються.

9. Суб'єкт платіжного ринку зобов'язаний:

1) розробити/доопрацювати внутрішні документи щодо інформаційної безпеки та кіберзахисту у сфері переказу коштів (далі – документи з кіберзахисту) з урахуванням вимог цього Положення та затвердити їх керівником, його заступником або керівним органом суб'єкта платіжного ринку (далі – керівництво);

2) підтримувати документи з інформаційної безпеки та кіберзахисту в актуальному стані та здійснювати їх перегляд не рідше одного разу на рік;

3) розмістити сервери, що використовуються для приймання, оброблення, передавання електронних документів на переказ, збереження архівів, та мережеве обладнання, що забезпечує захист їх внутрішньої мережі, у серверних приміщеннях на території України;

4) визначити та запровадити посилені вимоги до парольної політики для привілейованих облікових записів (довжина та складність паролів, частота зміни) та/або застосовувати багатофакторну автентифікацію для таких облікових записів;

5) забезпечити дотримання вимог до логінів та паролів, установлених у додатку 1 до цього Положення;

6) вжити заходів щодо обмеження використання програмного забезпечення (далі – ПЗ) та технічних пристроїв, розробником яких є юридична чи фізична особа-резидент держави-агресора;

7) забезпечити контроль за цілісністю клієнтського ПЗ, що реалізоване у вигляді програмного модуля, шляхом перевірки значень хеш-функцій на нього;

8) зберігати захищеними від несанкціонованого доступу (далі – НСД) облікові дані та паролі доступу до серверного і мережевого обладнання ключових суб'єктів платіжного ринку;

9) забезпечити неможливість створення HTML (HyperText Markup Language) – сторінки з вбудованим кодом, отриманим з інших веб-ресурсів, на своєму веб-сайті;

10) інформувати відвідувачів свого веб-сайта про перехід за зовнішнім посиланням у разі необхідності в переправленні (редиректі) на інший веб-сайт.

10. Керівництво суб'єкта платіжного ринку зобов'язане призначити особу(іб) та/або підрозділ(и), відповідальну(ий/их) за забезпечення інформаційної безпеки та кіберзахисту суб'єкта платіжного ринку, та здійснювати нагляд за її(їх) діяльністю.

Керівництво суб'єкта платіжного ринку несе відповідальність за виконання вимог із забезпечення інформаційної безпеки та кіберзахисту.

11. Особа(и) та/або підрозділ(и), відповідальна(і) за забезпечення інформаційної безпеки та кіберзахисту суб'єкта платіжного ринку здійснює(ють):

1) розроблення або беруть участь у розробленні документів з кіберзахисту суб'єкта платіжного ринку;

2) контроль за виконанням заходів щодо забезпечення інформаційної безпеки та кіберзахисту на всіх стадіях життєвого циклу (проектування, впровадження, експлуатація та виведення з експлуатації) інформаційних систем суб'єкта платіжного ринку;

3) моніторинг та розслідування інцидентів безпеки інформації та кіберінцидентів;

4) відновлення функціонування систем захисту інформаційних систем суб'єкта платіжного ринку після збоїв у роботі внаслідок інцидентів безпеки інформації та кіберінцидентів;

5) невідкладне повідомлення платіжної організації платіжної системи про:

виявлені вдалі чи невдалі спроби виконання шахрайських операцій;

виявлені фішингові веб-сайти;

компрометацію чи втрату ключів, паролів, засобів електронного підпису, засобів криптографічного захисту інформації.

12. Суб’єкт платіжного ринку під час вибору розрахункового банку повинен забезпечити виконання таких умов:

1) захист інформації, якою обмінюється процесингова установа з розрахунковим банком, здійснюється за допомогою сертифікованих ДССЗЗІ засобів криптографічного захисту інформації;

2) виконується автентифікація працівників процесингової установи за тією самою процедурою, що й для клієнтів банку;

3) створюється захищений мережевий канал із розрахунковим банком для захисту даних під час обміну електронними документами, що містять електронний підпис, який забезпечить перевірку цілісності, достовірності та авторства цих документів.

ІІІ. Порядок використання та адміністрування засобів захисту мережі

13. Суб’єкт платіжного ринку зобов’язаний використовувати засоби захисту мережі (апаратні та/або програмні), які мають чинний на момент початку експлуатації системи захисту мережі сертифікат відповідності або позитивний експертний висновок ДССЗЗІ, у випадках їх застосування для:

1) захисту мережевого з’єднання між компонентами суб’єкта платіжного ринку;

2) передавання між компонентами незашифрованої інформації без електронного підпису.

14. Засоби захисту мережі, передбачені пунктом 13 розділу ІІІ цього Положення, повинні відповідати Критеріям оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99, затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22 (зі змінами), а саме:

1) критеріям конфіденційності: адміністративна конфіденційність КА-1;

2) критеріям цілісності:
адміністративна цілісність ЦА-1;
відкат ЦО-2;

3) критеріям доступності:
використання ресурсів ДР-1;
стійкість до відмов ДС-1;

гаряча заміна ДЗ-2;
відновлення після збоїв ДВ-1;

4) критеріям спостережності:
реєстрація: НР-1;
ідентифікація і автентифікація НИ-1 або НИ-2;
достовірний канал НК-1;
розподіл обов'язків НО-2;
цілісність криптографічного захисту інформації НЦ-1;
автентифікація під час обміну НВ-1;

5) рівню гарантії: не нижче рівня Г-2.

15. Засоби захисту мережі, у разі їх використання для шифрування даних та/або створення електронного підпису електронних документів на переказ та їх архівів, повинні мати чинний на момент початку експлуатації системи захисту сертифікат відповідності або позитивний експертний висновок ДССЗЗІ, або NIST, або CEN.

16. Суб'єкт платіжного ринку зобов'язаний визначити перелік відповідальних осіб, що мають фізичний доступ до засобів захисту інформації.

Обов'язки адміністратора засобів захисту інформації повинні бути відокремлені від обов'язків адміністратора серверів баз даних та інших серверів захищеного сегмента.

17. Адміністратор засобів захисту мережі здійснює адміністрування одним із таких способів:

1) через консольний порт;

2) через захищений канал доступу з робочого місця адміністратора в контрольованій зоні;

3) із використанням надійних засобів для автентифікації адміністратора.

Доступ користувачів до компонентів, що перебувають у захищеному сегменті, допускається лише через засіб захисту мережі.

18. Суб'єкт платіжного ринку повинен забезпечити функціонування лише необхідних для роботи сервісів під час експлуатації засобу захисту інформації.

Оновлення внутрішнього ПЗ засобів захисту інформації мають право ініціювати лише визначені керівництвом суб'єкта платіжного ринку працівники.

19. Суб’єкт платіжного ринку зобов’язаний забезпечити можливість відміни внесених змін до системи конфігурації ПЗ та відновлення попередньої версії ПЗ засобів захисту інформації.

Внутрішнє ПЗ засобу захисту інформації повинно бути захищене від навмисної чи ненавмисної модифікації шляхом перевірки адміністратором контрольних сум цього ПЗ перед початком роботи.

20. Суб’єкт платіжного ринку зобов’язаний налаштувати засоби захисту мережі таким чином, щоб критичні дані під час передавання даних були захищені від несанкціонованого перегляду та модифікації.

До критичних даних належать:

1) електронні документи на переказ;

2) незашифровані та незахищені від модифікації дані, зчитані з електронного платіжного засобу;

3) логіни та паролі.

IV. Вимоги до суб’єкта платіжного ринку щодо взаємодії компонентів під час здійснення переказів коштів за участю двох платіжних систем

21. Суб’єкт платіжного ринку зобов’язаний забезпечити захист каналу обміну електронними повідомленнями та захист електронних документів за допомогою протоколу Hypertext Transfer Protocol Secure (далі – HTTPS) або шляхом створення віртуальної приватної мережі під час обміну інформаційними повідомленнями з іншим суб’єктом платіжного ринку чи з оператором послуг платіжної інфраструктури, що виконує роль посередника.

Суб’єкт платіжного ринку для HTTPS-з’єднання повинен використовувати криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS) версії не нижче 1.2 і сертифікат відкритого ключа веб-сервера, що відповідає вимогам, викладеним у пункті 29 розділу VI цього Положення.

Суб’єкт платіжного ринку повинен забезпечити налаштування віртуальної приватної мережі (Virtual private network, VPN) під час використання такої мережі для обміну інформацією відповідно до вимог, зазначених у розділі VI цього Положення.

22. Електронний документ щодо переказу коштів, що передається від однієї платіжної системи до іншої, повинен мати електронний підпис.

Договір між платіжними організаціями платіжних систем, які здійснюють перекази коштів між собою, повинен уключати порядок взаємного визнання електронних підписів, які засвідчують цілісність, достовірність та авторство електронного документа щодо переказу коштів.

23. Суб’єкт платіжного ринку зобов’язаний визначити порядок визнання електронного підпису на документах, створеного відповідальними особами нерезидента та відповідальною особою резидента, яка здійснює переказ коштів за допомогою оператора послуг платіжної інфраструктури-нерезидента, якщо через компоненти платіжної системи-резидента здійснюється обмін електронними документами з компонентами платіжної системи-нерезидента.

Оператор послуг платіжної інфраструктури-резидент, який забезпечує взаємодію з платіжною системою-нерезидентом, має право укласти договір із платіжною організацією платіжної системи-нерезидента про визнання електронного підпису. Оператор послуг платіжної інфраструктури-резидент зобов’язаний накласти свій електронний підпис на електронний документ відповідно до законодавства України після перевірки чинності електронного підпису платіжної системи-нерезидента.

V. Вимоги до суб’єкта платіжного ринку щодо створення та перевірки електронного підпису на електронних документах

24. Суб’єкт платіжного ринку зобов’язаний:

1) використовувати електронний підпис для забезпечення цілісності, достовірності та авторства електронних документів на переказ та архівів електронних документів на переказ;

2) створювати електронний підпис виключно за допомогою криптографічних засобів захисту інформації, що мають чинний позитивний експертний висновок ДССЗЗІ;

3) уключити до документів з кіберзахисту вимоги щодо захисту особистого ключа підписувача від НСД та несанкціонованого використання за допомогою криптографічних засобів захисту інформації або шляхом шифрування на всіх етапах його передавання і використання. Підписувач повинен використовувати пароль для забезпечення доступу до особистого ключа;

4) інформувати щодо результату оброблення електронного документа на переказ ініціатора цього переказу;

5) письмово попередити відповідальних осіб, які здійснюють накладання удосконаленого електронного підпису на електронний документ на переказ, про відповідальність за неналежну перевірку відправників та одержувачів платежів;

6) використовувати тільки ті криптографічні алгоритми та довжину криптографічних ключів, що зазначені в додатку 2 до цього Положення.

25. Суб'єкт платіжного ринку має право використовувати удосконалений електронний підпис без засвідчення чинності відкритого ключа у випадках, установлених законом, або за письмовою згодою суб'єкта платіжного ринку, у якій мають міститися зразки відповідного аналога власноручних підписів сторін правочину.

VI. Процедури генерації, розповсюдження, зберігання, використання та сертифікації криптографічних ключів

26. Суб'єкт платіжного ринку повинен здійснювати генерацію криптографічних ключів за допомогою надійних засобів. Засіб генерації криптографічного ключа, який використовується для створення електронного підпису на електронний документ на переказ або архіви електронних документів, повинен мати чинний позитивний експертний висновок ДССЗЗІ. Забороняється використання одного криптографічного ключа для різних цілей.

27. Суб'єкт платіжного ринку зобов'язаний розробити та затвердити методику відновлення та захисту зашифрованої інформації у випадках втрати, компрометації чи пошкодження криптографічних ключів або носіїв критичних даних.

28. Суб'єкт платіжного ринку під час розповсюдження, зберігання та використання криптографічних ключів зобов'язаний забезпечити:

1) захист криптографічних ключів від НСД чи пошкодження;

2) захист від неавторизованого розкриття особистих ключів асиметричних алгоритмів;

3) надання доступу до використання критичних даних, які зберігаються на апаратних криптографічних засобах захисту інформації, виключно після автентифікації власника ключа шляхом уведення ним секретного статичного чи динамічного коду доступу.

29. Суб'єкт платіжного ринку для виконання операцій з переказу коштів через захищене Інтернет-з'єднання, з метою підтвердження достовірності сервера повинен використовувати сертифікати відкритого ключа, видані центрами сертифікації, які забезпечують перевірку достовірності домену та організації (гарантійна сума сертифіката не може бути меншою 10 000 дол. США).

VII. Вимоги щодо забезпечення інформаційної безпеки та кіберзахисту ключовими суб’єктами платіжного ринку

30. Ключовий суб’єкт платіжного ринку для забезпечення інформаційної безпеки та кіберзахисту повинен виконувати вимоги, визначені в розділі VII цього Положення, та забезпечити належний контроль за їх виконанням.

31. Ключовий суб’єкт платіжного ринку зобов’язаний забезпечити захист платіжної інформації та критичних даних під час обміну з учасниками платіжної системи, а також під час оброблення та зберігання такої інформації.

32. Ключовий суб’єкт платіжного ринку зобов’язаний розмістити сервери, що здійснюють приймання, оброблення, передавання електронних документів на переказ, збереження архівів, та мережеве обладнання, що забезпечує захист їх внутрішньої мережі, у критичних приміщеннях на території України із забезпеченням виконання таких умов:

1) керівництвом ключового суб’єкта платіжного ринку визначено перелік відповідальних осіб, які мають доступ до критичного приміщення;

2) доступ до серверів заборонено без присутності відповідальних осіб ключового суб’єкта платіжного ринку;

3) приміщення обладнані охоронною сигналізацією;

4) ведеться реєстрація відвідувачів на вході до критичних приміщень шляхом занесення у журнал реєстрації інформації про осіб, що відвідували приміщення, дату і час входу та виходу, мету відвідування приміщення, установу, яку він представляє;

5) застосовуються засоби відеоспостереження для моніторингу відвідувань, сигналізація та автоматизовані засоби для розпізнавання порушень та ініціювання реагування на них;

6) заборонено розташування робочих місць працівників ключового суб’єкта платіжного ринку та сторонніх осіб у критичних приміщеннях;

7) використовуються безперебійні та резервні джерела живлення для захисту серверного та мережевого обладнання від збоїв в електроживленні;

8) приміщення обладнані системами протипожежного захисту;

9) заборонено використання мобільних та портативних пристроїв в режимі передавання даних;

10) заборонено використання безпровідних мереж шляхом застосування технічних пристроїв та адміністративних вимог;

11) здійснюється контроль за встановленням, видаленням чи заміною носіїв інформації на серверах;

12) обладнання ключового суб'єкта платіжного ринку розташовано в окремій серверній стійці, яка зачинена та опечатана, і доступ до якої мають лише відповідальні особи ключового суб'єкта платіжного ринку.

33. Ключовий суб'єкт платіжного ринку має право використовувати віртуальні сервери під управлінням гіпервізора з обов'язковим дотриманням таких вимог:

1) фізичні сервери, що забезпечують функціонування віртуальних серверів, розміщені в критичних приміщеннях, які відповідають вимогам пункту 32 розділу VII цього Положення;

2) обов'язки адміністратора віртуальних серверів та адміністратора гіпервізора не суміщено в одній посаді;

3) упроваджено політику безпеки налаштувань гіпервізора, які забезпечують захист гіпервізора та віртуальних серверів від НСД;

4) реєструються всі дії адміністраторів віртуальних серверів та гіпервізора;

5) здійснюється контроль за цілісністю налаштувань гіпервізора;

6) оновлення ПЗ гіпервізора виконується виключно адміністратором гіпервізора;

7) робочі місця адміністраторів, які здійснюють віддалене адміністрування віртуальних машин та гіпервізора, розміщуються в сегменті мережі, захищеному за допомогою засобів захисту інформації та організаційних заходів. З'єднання із використанням мереж загального користування захищено від несанкціонованого втручання та НСД за допомогою віртуальної приватної мережі;

8) гіпервізор, на якому працюють одна чи кілька віртуальних машин, захищено за допомогою окремого мережевого обладнання (фаєрвола, міжмережевого екрана) від зовнішнього несанкціонованого втручання;

9) файли образів віртуальних машин зберігаються в критичних приміщеннях, а їх передавання здійснюється виключно із забезпеченням конфіденційності та цілісності;

10) періодично зберігаються дані гіпервізора, необхідні для відновлення його працездатності.

34. Ключовий суб'єкт платіжного ринку має право використовувати хмарні технології/сервіси для забезпечення своєї діяльності за умови виконання таких вимог:

1) серверні приміщення компаній, які надають послуги хмарних технологій/сервісів, розташовані на території України та відповідають вимогам пункту 32 розділу VII цього Положення;

2) передавання образів віртуальних машин, копій баз даних із даними платежів та критичними даними до систем хмарних технологій/сервісів повинно здійснюватися в зашифрованому вигляді із використанням алгоритмів, наведених у додатку 2 до цього Положення.

35. Ключовий суб'єкт платіжного ринку має право використовувати системи хмарних технологій/сервісів на серверах, розміщених за межами України, лише для резервування інформації та за умови, що зберігання та обмін такою інформацією здійснюватиметься у зашифрованому вигляді із використанням алгоритмів, наведених у додатку 2 до цього Положення.

36. Ключовий суб'єкт платіжного ринку зобов'язаний визначити в посадових інструкціях працівників функції та обов'язки щодо розроблення, упровадження та підтримки політики безпеки в актуальному стані, виявлення, класифікації, реагування та аналізу інцидентів безпеки інформації та кіберінцидентів, а також обов'язки для працівників, які мають фізичний доступ до програмно-апаратних комплексів із оброблення та обміну інформацією, мережевого обладнання та комплексів із розроблення і тестування ПЗ.

Обов'язки та відповідальність за безпеку програмно-апаратних комплексів ключового суб'єкта платіжного ринку повинні розподілятися між різними підрозділами суб'єкта платіжного ринку.

37. Ключовому суб'єкту платіжного ринку заборонено суміщати такі посадові обов'язки:

1) адміністратора мережевого обладнання та адміністратора баз даних, працівників служб підтримки, експлуатації та супроводу функціонування системи;

2) працівників підрозділів розроблення, підтримки ПЗ та адміністратора баз даних, працівників служб підтримки, експлуатації, супроводу функціонування системи та тестування ПЗ;

3) адміністратора баз даних із працівниками з тестування ПЗ.

38. Ключовий суб'єкт платіжного ринку зобов'язаний розробити та затвердити технологічні інструкції, що регламентують:

1) виконання штатних процедур запуску та завершення роботи серверів;

2) виконання процедур резервного копіювання;

3) правила використання комп'ютерних приміщень;

4) використання та зберігання носіїв, що містять інформацію щодо документів на переказ та їх архівів.

39. Ключовий суб'єкт платіжного ринку зобов'язаний забезпечити захист інформації, що передається у його внутрішній мережі, від НСД шляхом виконання таких вимог:

1) доступ зовнішніх користувачів до веб-серверів та серверів, що забезпечують функціонування платіжних систем, здійснюється через єдину точку мережевого входу з використанням міжмережевого екрана;

2) міжмережевий екран контролює та фільтрує IP-адреси віддалених комп'ютерів і портів та IP-адреси у внутрішній мережі;

3) ведеться протоколювання з'єднань віддалених користувачів із міжмережевим екраном;

4) неможливий доступ до внутрішніх IP-адрес із мережі Інтернет;

5) заборонено використовувати на окремих компонентах внутрішньої мережі дротові та бездротові мережеві засоби, що можуть установлювати з'єднання з мережами загального користування в обхід міжмережевого екрана, та будувати внутрішню мережу з використанням бездротових технологій;

6) робочі місця адміністраторів мережевого обладнання та серверів використовуються лише для виконання їх посадових обов'язків. Заборонено встановлювати на таких робочих місцях клієнтів електронної пошти та іншого ПЗ, що використовує з'єднання з мережами загального користування;

7) мережі серверів та обладнання, що забезпечує функціонування сервісів, відкритих для доступу клієнтів із публічної мережі, повинні розміщуватися в демілітаризованій зоні;

8) внутрішня мережа ключового суб'єкта платіжного ринку, що здійснює оброблення інформації щодо переказу коштів, повинна бути захищена від зовнішнього втручання за допомогою програмно-апаратних або програмних засобів;

9) захист інформації, якою обмінюються сервери програмно-апаратних комплексів ключового суб'єкта платіжного ринку, розміщені в різних приміщеннях та об'єднані за допомогою мереж загального користування, забезпечується шляхом шифрування каналу обміну з використанням криптографічних ключів, які не можуть бути перехоплені сторонніми особами;

10) доступ до веб-серверів, розміщених у захищеній зоні, здійснюється за допомогою засобів захисту інформації. Інші суб'єкти платіжного ринку не мають доступу до інших компонентів ключового суб'єкта платіжного ринку;

11) установлення захищеного з'єднання зовнішніх користувачів із веб-серверами здійснюється з використанням захищеного протоколу HTTPS з криптографічним протоколом захисту на транспортному рівні (Transport layer security, TLS) версії не нижче 1.2 та сертифікатом відкритого ключа веб-сервера, що відповідає вимогам, викладеним у пункті 29 розділу VI цього Положення;

12) віртуальною приватною мережею здійснюється захист інформації за допомогою надійних симетричних алгоритмів шифрування, зазначених у додатку 2 до цього Положення, мережевого протоколу IPSec [представницький рівень мережевої моделі Open Systems Interconnection, OSI повинен мати протокол захисту транспортного рівня (Transport layer security, TLS) версії не нижче 1.2];

13) тестування на проникнення виконується не рідше одного разу на рік.

40. Міжмережевий екран, реалізований програмними засобами, повинен розміщуватися на окремому сервері та мати чинний позитивний експертний висновок ДССЗЗІ про відповідність вимогам щодо захисту інформації в Україні на рівні не нижчому, ніж зазначений у пункті 14 розділу III цього Положення.

Ключовий суб'єкт платіжного ринку зобов'язаний своєчасно встановлювати актуальні оновлення ПЗ міжмережевого екрана.

Ключовому суб'єкту платіжного ринку заборонено використовувати сервери, що застосовуються для цілей маршрутизації з будь-якою іншою метою.

41. Ключовий суб’єкт платіжного ринку зобов’язаний забезпечити:

1) створення облікових записів адміністратора та користувачів під час налаштування операційних систем. Паролі до облікових записів повинні відповідати вимогам, зазначеним у додатку 1 до цього Положення;

2) дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем (уключаючи доступ привілейованих користувачів);

3) обмеження та контроль за використанням системних утиліт;

4) ідентифікацію користувачів у разі віддаленого доступу інформаційних систем ключового суб’єкта платіжного ринку;

5) блокування облікового запису адміністратора чи користувача в разі п’яти невдалих спроб автентифікації поспіль (автоматичне блокування). Подальше розблокування доступу можливе лише за результатами внутрішнього розслідування ключовим суб’єктом платіжного ринку;

6) використання операційних систем, які підтримуються розробником, та вчасне встановлення необхідних оновлень, що усувають виявлені вразливості;

7) своєчасне встановлення актуальних оновлень ПЗ міжмережевого екрана;

8) протоколювання (ведення операційними системами деталізованих електронних журналів) усіх дій щодо надання, скасування чи зміни доступу користувачів в операційній системі, що реєструють:
унікальні ідентифікатори користувачів;
дату та час входу користувача в операційну систему та виходу з неї;
ідентифікатор віддаленого робочого місця чи термінала;
результат успішності спроби входу в операційну систему.

42. Ключовий суб’єкт платіжного ринку зобов’язаний використовувати для оброблення платіжних документів ПЗ, що має технічну підтримку від розробників або створене і підтримується безпосередньо ключовим суб’єктом платіжного ринку. У разі виявлення помилок, що ускладнюють або унеможливлюють виконання передбачених функцій, технічною підтримкою повинно бути передбачено можливість усунення виявлених недоліків та надання нових версій ПЗ, що успішно пройшли випробування в тестовому середовищі.

Тестове середовище повинно відокремлюватися від середовища промислової експлуатації, а працівники, які вносять зміни до ПЗ, не повинні мати можливості працювати в середовищі промислової експлуатації.

43. Відповідальна особа ключового суб'єкта платіжного ринку зобов'язана здійснювати контроль за цілісністю та версіями ПЗ, яке експлуатується.

Засоби криптографічного захисту інформації, що використовуються ПЗ, яке експлуатується ключовим суб'єктом платіжного ринку, повинні мати чинний сертифікат та/або позитивний експертний висновок у сфері криптографічного захисту інформації однієї з таких установ: ДССЗЗІ, NIST або CEN.

Засоби криптографічного захисту інформації, які використовуються ключовим суб'єктом платіжного ринку для захисту інформації, вимоги щодо захисту якої встановлено законодавством України, повинні мати чинний позитивний експертний висновок ДССЗЗІ.

44. Ключовий суб'єкт платіжного ринку повинен забезпечити автентифікацію адміністраторів із виконанням хоча б однієї з таких вимог:

1) з робочого місця в захищеному сегменті;

2) за допомогою додаткових дозволів на автентифікацію;

3) із забезпеченням реалізації правила "двох рук" (коли автентифікація не може бути ініційована та виконана однією відповідальною особою).

45. Ключовий суб'єкт платіжного ринку зобов'язаний забезпечити відповідність серверного ПЗ, доступ до якого мають користувачі, таким вимогам:

1) ведеться захищений від несанкціонованого втручання журнал операцій, що фіксує ідентифікатор (логін, ім'я, телефонний номер), дату і час, назву операції, результат операції та додаткові дані, що дають змогу ідентифікувати операцію;

2) передбачено граничний час неактивності для користувачів ПЗ, який не повинен перевищувати 60 хвилин, після якого сеанс роботи з ПЗ повинен бути закритим;

3) усі користувачі, для яких передбачено можливість використання певних функціональних можливостей серверного ПЗ, проходять автентифікацію;

4) пароль користувача не повинен передаватися через незахищені мережі у відкритому вигляді та повинен зберігатися в базах даних шляхом збереження замість нього дозволених цим Положенням хеш-функцій від об'єднання пароля з випадковим числом, попередньо надісланим користувачу, або іншим

аналогічним чином. У цьому разі користувачі повинні мати змогу змінювати свій пароль;

5) серверне ПЗ здійснює ідентифікацію користувача шляхом перевірки його удосконаленого електронного підпису за умови, якщо відкритий ключ надано власником особисто та встановлено особу власника;

6) віддалені користувачі, які здійснюють переказ коштів, проходять багатофакторну автентифікацію;

7) заборонено використовувати соціальні мережі та інші веб-сервіси загального користування для автентифікації користувачів;

8) серверне ПЗ повинно мати базовий механізм розмежування доступу для різних користувачів шляхом визначення необхідного переліку ролей, кожна з яких повинна давати змогу користувачам виконувати визначені переліком функції та мати права доступу, необхідні для виконання цих функцій;

9) роль адміністратора повинна забезпечувати можливість створювати в цьому ПЗ облікові записи інших користувачів, здійснювати модифікацію прав доступу цих користувачів, а також здійснювати відключення чи видалення їх облікових записів;

10) розроблено та затверджено регламент, відповідно до якого повинні видалятися облікові записи користувачів та їх ролі, що втратили актуальність;

11) ПЗ має модуль диспетчера доступу, який аналізує запити від користувачів, проводить їх автентифікацію та забезпечує доступ до виконання лише тих функцій, на які має право конкретний користувач із конкретною роллю;

12) ПЗ, що використовується ключовим суб’єктом платіжного ринку для забезпечення функціонування платіжних систем та систем розрахунків, повинно бути захищене від НСД, збоїв, у ньому повинні бути усунуті всі відомі на момент випробувань вразливості;

13) перед упровадженням у дослідну чи промислову експлуатацію ПЗ повинно пройти функціональні випробування та перевірку вихідних текстів фахівцями, незалежними від розробників, або зовнішньою аудиторською компанією.

46. Ключовий суб’єкт платіжного ринку з метою захисту від НСД до даних та програмно-апаратних комплексів зобов’язаний:

1) визначити перелік можливих загроз НСД під час побудови системи захисту інформації та вжити заходів для їх усунення;

2) забезпечити інформаційну безпеку та кіберзахист серверів від несанкціонованого втручання та НСД шляхом використання апаратних та/або програмних засобів;

3) забезпечити доступ до баз даних та електронних журналів у режимі читання, запису та знищення інформації лише уповноваженим особам.

47. Відповідальна особа ключового суб'єкта платіжного ринку з метою уникнення встановлення на серверному обладнанні шкідливого ПЗ зобов'язана:

1) установити на сервери та робочі станції лише те ПЗ, яке необхідне для виконання поставлених завдань, та регулярно переглядати перелік такого ПЗ;

2) налаштувати права користувачів, які працюють на робочих станціях та серверах, таким чином, щоб вони обмежувалися лише виконанням посадових обов'язків;

3) упровадити політику обмеження використання змінних носіїв інформації;

4) упровадити спеціалізовані програмні засоби контролю для виявлення і попередження проникнення шкідливих програм;

5) установити та регулярно оновлювати антивірусне ПЗ для сканування серверів, робочих станцій та змінних носіїв інформації на шкідливе ПЗ;

6) здійснювати моніторинг спроб несанкціонованої зміни ПЗ та блокувати такі спроби.

48. Керівництво ключового суб'єкта платіжного ринку зобов'язане попередити відповідальну особу ключового суб'єкта платіжного ринку про неприпустимість використання шкідливого ПЗ та ПЗ із порушенням авторського права.

49. Ключовий суб'єкт платіжного ринку з метою забезпечення безперервної діяльності платіжної системи зобов'язаний:

1) забезпечити наявність не менше одного резервного програмно-апаратного комплексу для забезпечення безперервної діяльності платіжної системи або системи розрахунків. Вимоги до розміщення такого комплексу

повинні відповідати вимогам до розміщення основного комплексу, водночас основний та резервний комплекси повинні бути територіально рознесені;

2) розробити методику та затвердити регламент контролю за працездатністю резервного обладнання;

3) здійснювати резервування стану операційної системи для швидкого відновлення роботи серверів. Фізичні носії інформації, що містять резервні копії, повинні бути захищені від НСД та шкідливого зовнішнього впливу, розміщуватися в критичних приміщеннях, відмінних від приміщення, де розміщено програмно-апаратні комплекси ключового суб'єкта платіжного ринку.

Передавання резервної копії повинно здійснюватися через захищені лінії зв'язку зі створенням VPN-каналу або шляхом транспортування носія інформації відповідальною особою;

4) вести облік фізичних носіїв інформації, що містять резервні копії, та місць їх зберігання. Кожен носій інформації після запису на нього резервної копії повинен запечатуватися та заклеюватися в окремому конверті із зазначенням на ньому такої інформації:

виду інформації, що міститься на носії;

посади, прізвища та ініціалів працівника, який записав резервну копію;

дати та часу запису резервної копії;

типу носія інформації;

5) розробити та затвердити процедури відновлення роботи серверів із використанням резервних копій. Тестування такого відновлення ключовим суб'єктом платіжного ринку повинно здійснюватися не рідше одного разу на рік;

6) розробити та затвердити регламент перевірки цілісності та працездатності резервних копій;

7) переглядати затверджену процедуру створення резервних копій під час унесення змін до ПЗ або апаратної платформи.

50. Ключовий суб'єкт платіжного ринку зобов'язаний протоколювати дії з видалення неактуальних архівів та образів із зазначенням такої інформації:

1) дати та часу події;

2) унікального ідентифікатора користувача, який ініціював видалення;

3) результату дії (успіх або невдача).

51. Фізичний носій інформації, що виводиться з експлуатації, повинен знищуватися відповідальною особою ключового суб'єкта платіжного ринку із попереднім видаленням на ньому усієї інформації гарантованими засобами зі складанням акта про знищення інформації.

52. Ключовий суб'єкт платіжного ринку зобов'язаний забезпечити резервування інформації, що містить електронні документи на переказ уключно з електронними підписами, з можливістю їх відновлення та перевірки цілісності, достовірності та авторства документів на переказ.

Фізичні носії, де зберігаються резервні копії електронних архівів, повинні бути захищені від НСД та зберігатися в критичному приміщенні.

53. Періодичність збереження архівів електронних документів на переказ не повинна перевищувати строк збереження журналів та файлів, призначених для відновлення операцій в платіжній системі.

54. Ключовий суб'єкт платіжного ринку для мінімізації можливих збитків від кіберінцидентів у системах захисту інформації та порушень функціонування програмно-апаратних комплексів, що здійснюють оброблення документів на переказ, зобов'язаний:

1) здійснювати моніторинг за функціонуванням програмно-апаратних комплексів щодо порушень інформаційної безпеки та кіберзахисту;

2) проводити аналіз здійснення платежів з метою виявлення статистично недостовірних операцій;

3) установити порядок постійного моніторингу, реєстрації та документування інцидентів кібербезпеки щодо порушення роботи систем захисту інформації;

4) використовувати автоматизовані засоби відслідковування, збору та аналізу інформації про інциденти кібербезпеки;

5) розробити, упровадити та періодично оновлювати політику реагування на кіберінциденти, а також план заходів щодо реалізації політики реагування на інциденти щодо порушення роботи систем захисту інформації;

6) повідомляти Національний банк про виявлені кіберінциденти або вразливості у функціонуванні платіжної системи, системи розрахунків засобами електронної пошти Національного банку (у разі підключення) або іншими узгодженими засобами електронного зв'язку;

7) невідкладно повідомити Національний банк та правоохоронні органи в разі виявлення кібератак, що знижують надійність функціонування платіжної системи, системи розрахунків або уможливлюють здійснення шахрайських операцій;

8) установити дисциплінарну відповідальність працівників за порушення вимог із забезпечення інформаційної безпеки та кіберзахисту внутрішнім розпорядчим документом;

9) проводити навчання відповідальних осіб за забезпечення інформаційної безпеки та кіберзахисту з питань запобігання, виявлення порушень роботи систем захисту та усунення їх наслідків.

Директор
Департаменту безпеки О. А. Скомаровський

Додаток 1
до Положення про кіберзахист
та інформаційну безпеку в платіжних
системах та системах розрахунків
(підпункт 5 пункту 9 розділу II)

Вимоги до логінів та паролів

1. Логіни та паролі користувачів платіжних послуг, учасників платіжних систем та систем розрахунків створюються під час реєстрації.

2. Передавання паролів здійснюється в захищеному від перегляду та модифікації вигляді.

3. Пароль може передаватися через мережі загального користування (електронна пошта, електронні повідомлення) за таких умов:

1) із застосуванням багатофакторної автентифікації;

2) короткий термін використання пароля (не більше 30 хвилин);

3) пароль дійсний для одноразового використання.

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 інформаційну безпеку та кіберзахист 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.

7. Заборонено записувати паролі на паперових чи електронних носіях у відкритому вигляді, якщо не забезпечено їх зберігання від НСД.

Додаток 2
до Положення про кіберзахист
та інформаційну безпеку в платіжних
системах та системах розрахунків
(підпункт 6 пункту 24 розділу V)

Криптографічні алгоритми та довжина криптографічних ключів

1. Симетричні криптографічні алгоритми

Таблиця 1

№ з/п	Алгоритм	Умови застосування	Довжина ключа, біт
1	2	3	4
1	Triple Data Encryption Algorithm, TDES (TDEA)	Довготривале використання	112
2	Advanced Encryption Standard, AES	Довготривале використання	128, 192, 256
3	Serpent	Довготривале використання	128, 192, 256
4	Twofish	Довготривале використання	128, 192, 256
5	Blowfish	Довготривале використання	Не менше 144
6	International Data Encryption Algorithm, IDEA	Захист мережі	128
7	ChaCha20	Захист мережі (потоковий)	256
8	Національний стандарт України ДСТУ ГОСТ 28147:2009 “Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования”, затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495 “Про прийняття міждержавних стандартів як національні методом підтвердження та скасування відповідних міждержавних стандартів”	Довготривале використання	256

Продовження додатка 2
Продовження таблиці 1

1	2	3	4
9	Національний стандарт України ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”, затверджений наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484 “Про прийняття нормативних документів України та пробних національних стандартів України, гармонізованих з міжнародними нормативними документами, міжнародного та європейських стандартів як національних стандартів України, затвердження національних стандартів України, скасування національних стандартів України та міждержавних стандартів в Україні”	Довготривале використання	128, 256, 512

2. Асиметричні криптографічні алгоритми

Таблиця 2

№ з/п	Алгоритм	Умови застосування	Довжина ключа, біт
1	2	3	4
1	RSA (Rivest, Shamir и Adleman PKCS #1 v.2.2 RSA Cryptography Standart RSA Laboratory 27.10.2012)	Удосконалений електронний підпис. Довготривале використання. Термін використання не більше двох років	1024, 2048, 4096
2	Digital Signature Algorithm, DSA	Удосконалений електронний підпис	1024, 2048, 3072

Продовження додатка 2
Продовження таблиці 2

1	2	3	4
3	Elliptic Curve Digital Signature Algorithm, ECDSA	Удосконалений електронний підпис (крім документів на переказ та архівів)	160
4	ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, затверджений наказом Державного комітету Україні з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31	Удосконалений електронний підпис	163, 167, 173, 179, 191, 233, 257, 307, 367, 431 (поліноміальний базис) та 173, 179, 191, 233, 431 (оптимальний нормальний базис)

3. Хеш-функції

Таблиця 3

№ з/п	Алгоритм	Умови застосування	Довжина ключа, біт
1	2	3	4
1	SHA-2, FIPS PUB 180-4 Secure Hash Standard	Перевірка цілісності. Захист каналів	224 (SHA-224), 256 (SHA-256), 384 (SHA-384), 512 (SHA-512)
2	SHA-3, FIPS PUB 202 SHA-3 Standard	Перевірка цілісності. Захист каналів	224, 256, 384, 51
3	Міждержавний стандарт ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”, затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640	Перевірка цілісності. Захист каналів	256

Продовження додатка 2
Продовження таблиці 3

1	2	3	4
4	Національний стандарт ДСТУ 7564-2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”, затверджений наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431 “Про прийняття національних стандартів України, гармонізованих з європейськими стандартами, міжнародних стандартів як національних стандартів України, затвердження національних стандартів України, скасування міждержавних стандартів в Україні та внесення зміни до наказу Державного комітету стандартизації, метрології та сертифікації України від 12.06.2002 № 357”	Перевірка цілісності. Захист каналів	8 – 512
5	Message authentication code, MAC	Електронний підпис	Залежно від алгоритму