ПРОЄКТ

Правління Національного банку України

П О С Т А Н О В А

м. Київ №

Про затвердження Положення про захист інформації
та кіберзахист в 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 із забезпечення захисту інформації та кіберзахисту в платіжних системах та системах розрахунків Правління Національного банку України **постановляє:**

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

2. Платіжним організаціям платіжних систем, учасникам/членам платіжних систем та операторам послуг платіжної інфраструктури протягом 12 місяців з моменту набрання чинності Положенням:

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 (Олександр Скомаровський) 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

Положення
про захист інформації та кіберзахист
в 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 захист інформації в інформаційно-телекомунікаційних системах”, “Про інформацію”, “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 вимоги до захисту інформації та кіберзахисту в сфері переказу коштів з метою забезпечення інформаційної безпеки та кібербезпеки.

3. 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 (далі – керівництво) відповідальна особа, яка забезпечує процеси супроводу та управління програмними та/або апаратними засобами чи ресурсами;

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 реалізовує паралельне виконання кількох віртуальних машин на одному комп’ютері, забезпечуючи ізоляцію цих віртуальних машин та можливість керування

наявними ресурсами, зокрема можливість розподілення ресурсів між використовуваними віртуальними машинами;

5) засіб захисту мережі – програмний чи апаратний засіб, який захищає комп'ютерну мережу від несанкціонованого доступу до її складових, випадкового або навмисного втручання в роботу мережі;

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

7) ключовий суб'єкт платіжного ринку – суб'єкт платіжного ринку, який належить до однієї або більше категорії:

платіжна організація значущої платіжної системи, якщо вона виконує функції оператора послуг платіжної інфраструктури,

значущий оператор послуг платіжної інфраструктури,

оператор послуг платіжної інфраструктури, який обслуговує платіжну систему, створену нерезидентом,

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

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

9) 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;

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

11) надійні засоби – криптографічні засоби захисту інформації, що мають чинний на момент початку експлуатації сертифікат відповідності або позитивний експертний висновок за результатами експертизи у сфері захисту інформації, виданий одним з таких органів: Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок), Національного інституту стандартів та технологій Сполучених Штатів Америки (NIST);

12) 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 даної інформації без згоди (дозволу) керівництва чи уповноважених ним осіб;

13) суб'єкти платіжного ринку – це платіжні організації платіжних систем, створені резидентами України, учасники - резиденти платіжних систем (далі – учасники платіжних систем), створені резидентами, учасники платіжних систем,

створені нерезидентами, (крім поширення вимог щодо використання цими учасниками засобів захисту інформації відповідно до правил цих платіжних систем та з урахування вимог юрисдикцій, де їхні правила були узгоджені), оператори послуг платіжної інфраструктури (в разі надання інших видів послуг, крім оброблення інформації за операціями в міжнародних карткових платіжних системах);

14) технологія хмарних обчислень – технологія забезпечення доступу до хмарної інфраструктури через електронні комунікаційні мережі.

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

4. Дія цього Положення поширюється на суб'єктів платіжного ринку.

5. Вимоги цього Положення поширюються виключно на такі активи суб’єктів платіжного ринку, пов’язані з переказом коштів:

1) електронні документи на переказ;

2) інформаційні повідомлення між суб’єктами платіжного ринку, пов’язані з переказом коштів;

3) бази даних, що містять інформацію щодо переказу коштів;

4) серверне та мережеве обладнання, задіяне для переказу коштів;

5) технічні та криптографічні засоби захисту інформації;

6) криптографічні ключі.

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

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

7. Суб’єкт платіжного ринку забезпечує виконання вимог цього Положення щодо програмних, апаратних засобів і комплексів, мережевого обладнання, які ним використовуються.

8. Керівник суб’єкта платіжного ринку здійснює загальну організацію діяльності з питань забезпечення захисту інформації, інформаційної безпеки та кіберзахисту.

З цією метою керівник суб’єкту платіжного ринку:

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

2) затверджує політику інформаційної безпеки, а також інші документи з питань захисту інформації, інформаційної безпеки та кіберзахисту;

3) письмово попереджує осіб, які здійснюють накладання удосконаленого електронного підпису на електронний документ на переказ, про відповідальність за неналежну перевірку відправників та одержувачів переказу коштів.

9. Відповідальні особи за забезпечення захисту інформації, інформаційної безпеки та кіберзахисту суб'єкта платіжного ринку:

1) забезпечують виконання вимог цього Положення;

2) здійснюють 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, що використовуються для переказу коштів;

3) розробляють політики інформаційної безпеки, а також інші документи з питань захисту інформації, інформаційної безпеки та кіберзахисту;

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

5) здійснюють контроль працездатності засобів захисту інформації, організовують відновлення їх працездатності у випадку порушення функціонування.

6) здійснюють контроль складу та цілісності програмних та апаратних засобів захисту інформаційних систем, що використовуються для переказу коштів, вживають заходів щодо недопущення встановлення та використання у складі інформаційних систем програмних і апаратних засобів, не передбачених документами з питань захисту інформації, інформаційної безпеки та кіберзахисту;

7) погоджують можливість модернізації інформаційних систем, що використовуються для переказу коштів, з урахуванням вимог законодавства та правил платіжних систем у частині питань захисту інформації, інформаційної безпеки та кіберзахисту;

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

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

10. Суб'єкт платіжного ринку повинен розробити такі внутрішні документи з питань захисту інформації, інформаційної безпеки та кіберзахисту:

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

2) інструкції, що встановлюють повноваження та відповідальність персоналу з питань забезпечення захисту інформації, інформаційної безпеки та кіберзахисту, у тому числі відповідальної особи;

3) вимоги щодо захисту особистих ключів підписувачів від НСД;

4) порядок визнання електронного підпису на документах на переказ у разі здійснення учасником платіжної системи-нерезидента переказу коштів з використанням надійних засобів платіжної системи-нерезидента;

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

До критичних даних належать:

електронні документи на переказ,

незашифровані та незахищені від модифікації дані, які отримані з електронного платіжного засобу,

паролі,

персональні дані,

архіви цих даних;

6) вимоги до паролів, що не суперечать вимогам, визначеним у додатку 1 до цього Положення;

7) політику реагування на інциденти інформаційної безпеки та кіберінциденти.

11. Ключовий суб’єкт платіжного ринку зобов’язаний розробити такі документи:

1) порядок виконання процедур резервного копіювання електронних документів на переказ та даних, необхідних для відновлення функціонування суб’єкта платіжного ринку;

2) регламент перегляду облікових записів користувачів та їхніх ролей з метою підтримки їх в актуальному стані;

3) політику обмеження використання змінних носіїв інформації;

4) процедуру створення резервних копій під час унесення змін до програмного забезпечення (далі – ПЗ) або апаратних засобів і комплексів, мережевого обладнання;

5) регламент перевірки цілісності та працездатності резервних копій;

6) процедури відновлення роботи серверів із використанням резервних копій;

7) політику захисту від шкідливого ПЗ, зловмисного коду та вірусів.

12. Документи, зазначені у пунктах 11, 12 розділу ІІІ цього Положення, можуть бути оформлені як розділи одного документу. Перегляд внутрішніх документів з питань захисту інформації, інформаційної безпеки та кіберзахисту здійснюється за необхідності, але не рідше одного разу на рік.

13. Суб’єкт платіжного ринку застосовує технології хмарних обчислень для переказу коштів відповідно до порядку та вимог, що визначаються Національним банком.

IV. Фізичний захист

14. Суб'єкт платіжного ринку зобов’язаний забезпечити розміщення серверів, що використовуються для зберігання та обробки електронних документів на переказ, персональних даних користувачів та архівів цих даних, у критичних приміщеннях. Перелік працівників суб’єкта платіжного ринку, яким надається право постійного доступу до критичних приміщень, визначається відповідальною особою та затверджується керівником суб’єкта або його заступником. Доступ інших осіб до критичних приміщень надається за погодженням з відповідальною особою та у присутності працівників, яким надається право постійного доступу до цих приміщень.

Суб'єкт платіжного ринку у випадку використання серверного та мережевого обладнання на умовах оренди визначає порядок доступу до цього обладнання на договірних засадах з урахуванням вимог цього положення.

15. Критичні приміщення мають відповідати таким вимогам:

1) обладнані технічними засобами, що використовуються під час провадження охоронної діяльності: системи, прилади та обладнання для виявлення та попередження небезпеки для людей та\або майна, а також системи оповіщення про наявність такої небезпеки;

2) застосовуються засоби відеоспостереження для моніторингу відвідувань;

3) не допускається розташування робочих місць;

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

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

6) заборонено використання безпровідних мереж шляхом застосування технічних пристроїв та організаційних вимог;

7) здійснюється контроль за встановленням, видаленням чи заміною носіїв інформації на серверах.

V. Ідентифікація та автентифікація

16. Суб'єкту платіжного ринку забороняється здійснювати ідентифікацію та автентифікацію до засобів захисту з використанням даних, що встановлені за замовчуванням виробником обладнання.

17. Усі користувачі, для яких передбачено можливість віддаленого використання певних функціональних можливостей серверного ПЗ ключового суб’єкта платіжного ринку повинні проходити автентифікацію, що відповідає таким умовам:

1) пароль користувача не повинен передаватися через незахищені мережі у відкритому вигляді та повинен зберігатися в базах даних шляхом збереження замість нього значень дозволених цим Положенням ґеш-функцій від об’єднання пароля з випадковим числом. Користувачі повинні мати змогу змінювати свій пароль;

2) удосконалений електронний підпис користувача може використовуватись прикладним серверним ПЗ для автентифікації лише у випадку, коли відкритий ключ був наданий користувачем ключового суб'єкта платіжного ринку особисто та особу власника ключа перевірено;

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

4) заборонено використовувати соціальні мережі та інші веб-сервіси загального користування для автентифікації користувачів.

VI. Управління доступом

18. Суб'єкт платіжного ринку зобов'язаний забезпечити розробку, документування та періодичне оновлення політики управління доступом, а також заходів, пов'язаних з реалізацією цієї політики. Політика управління доступом має визначати:

1) порядок створення, активації, модифікації, перегляду, блокування, відключення, видалення, контролю використання облікових записів користувачів, типи облікових записів в залежності від категорії користувачів;

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

3) правила розмежування доступу користувачів.

19. Ключовий суб'єкт платіжного ринку зобов'язаний забезпечити захист інформації щодо переказу коштів, 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 засобу захисту мережі;

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

3) ведеться протоколювання з'єднань віддалених користувачів із засобом захисту мережі;

4) неможливий доступ до внутрішніх IP-адрес із мереж загального користування;

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

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

7) захист інформації, якою обмінюються сервери програмно-апаратних комплексів ключового суб'єкта платіжного ринку, що 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;

8) забезпечено захист від НСД облікових даних та паролів доступу до серверного і мережевого обладнання ключових суб'єктів платіжного ринку.

VII. Захист від шкідливого ПЗ, зловмисного коду та вірусів

20. Суб'єкт платіжного ринку зобов'язаний забезпечити захист 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 компонентів цього ПЗ, дозволених до використання в інформаційних системах, що використовуються для переказу коштів;

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

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

5) обмеження переліку компонентів ПЗ, що запускаються автоматично при завантаженні операційних систем інформаційних систем;

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

21. Суб'єкт платіжного ринку зобов'язаний попередити своїх працівників про неприпустимість використання шкідливого ПЗ та ПЗ із порушенням авторського права.

VIII. Забезпечення мережевого захисту

22. Суб’єкт платіжного ринку зобов’язаний використовувати засоби захисту мережі (апаратні та/або програмні), які мають чинний на момент початку експлуатації системи захисту мережі позитивний експертний висновок або сертифікат відповідності вимогам нормативних документів системи технічного захисту інформації в Україні Держспецзв’язку, виключно у випадках їх застосування для передавання між компонентами:

1) електронних документів на переказ без електронного підпису;

2) криптографічних ключів та паролів, незашифрованих за допомогою інших засобів.

23. Суб’єкт платіжного ринку для шифрування інформації з обмеженим доступом, що не перерахована в пункті 22 розділу VIII цього Положення, повинен використовувати надійні засоби.

24. Адміністратор засобів захисту мережі суб’єкта платіжного ринку здійснює адміністрування одним із таких способів:

1) через консольний порт;

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

25. Суб’єкт платіжного ринку при експлуатації засобу захисту мережі повинен:

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

2) забезпечити можливість скасування внесених змін 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).

26. Ключовий суб’єкт платіжного ринку при експлуатації засобу захисту мережі зобов’язаний:

1) забезпечити своєчасне встановлення актуальних оновлень внутрішнього ПЗ засобу захисту мережі;

2) не використовувати сервери, що застосовуються для цілей маршрутизації, з будь-якою іншою метою.

27. Суб’єкт платіжного ринку у випадку створення віртуальної приватної мережі для обміну критичними даними повинен використовувати лише криптографічні алгоритми шифрування, зазначені у додатку 2 до цього Положення.

IX. Вимоги до управління конфігурацією інформаційних систем та до забезпечення її цілісності.

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

29. Суб’єкту платіжного ринку при проектуванні та використанні своїх інформаційних систем забороняється використання ПЗ та технічні пристрої, розробником та/або виробником яких є юридична чи фізична особа, що включена до санкційних списків Ради національної безпеки і оборони України.

30. Ключовий суб’єкт платіжного ринку зобов’язаний забезпечити блокування облікового запису адміністратора чи користувача в разі шести невдалих спроб автентифікації поспіль (автоматичне блокування).

X. Вимоги до криптографічних засобів захисту інформації та середовища віртуалізації

31. Суб’єкт платіжного ринку повинен забезпечити виконання таких вимог:

1) засоби криптографічного захисту інформації, що використовуються для захисту інформації, вимога щодо захисту якої встановлена законом, повинні мати чинний на момент початку експлуатації сертифікат відповідності або позитивний експертний висновок Держспецзв’язку;

2) особисті ключі підписувача та ключі симетричних алгоритмів шифрування мають бути захищеними від НСД та несанкціонованого використання за допомогою криптографічних засобів захисту інформації, зокрема шляхом шифрування на всіх етапах його передавання і використання;

3) використовуються тільки ті криптографічні алгоритми та довжини криптографічних ключів, що зазначені в додатку 2 до цього Положення;

4) забезпечується контроль за цілісністю криптографічних бібліотек шляхом перевірки значень ґеш-функцій від них.

32. Ключовий суб’єкт платіжного ринку має право використовувати для переказу коштів віртуальні сервери під управлінням гіпервізора з обов’язковим дотриманням таких вимог:

1) фізичні сервери, що забезпечують функціонування віртуальних серверів, розміщені в критичних приміщеннях;

2) реєструються всі дії адміністраторів віртуальних серверів та гіпервізора;

3) здійснюється контроль за цілісністю налаштувань гіпервізора;

4) оновлення ПЗ гіпервізора виконується виключно адміністратором гіпервізора;

5) гіпервізор, на якому працюють одна чи кілька віртуальних машин, захищено за допомогою засобу захисту мережі від зовнішнього НСД;

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

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

XI. Вимоги до використання електронного підпису

33. Оператор послуг платіжної інфраструктури, 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 зобов’язаний накласти свій електронний підпис на електронний документ на переказ відповідно до законодавства України після перевірки чинності електронного підпису платіжної системи-нерезидента.

34. Суб’єкт платіжного ринку має право використовувати удосконалений електронний підпис без сертифіката відкритого ключа або чинність відкритого ключа підписувача засвідчується сертифікатом відкритого ключа на договірних засадах.

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

35. Суб’єкт платіжного ринку зобов’язаний забезпечити розробку, документування та періодичне оновлення політики управління інцидентами, а також заходів, пов’язаних з реалізацією цієї політики. Політика управління інцидентами має містити:

1) перелік та класифікація подій, що відносять до порушень інформаційної безпеки, інцидентів інформаційної безпеки та кіберінцидентів (далі – події);

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

3) порядок реагування на події у разі їх виникнення;

4) порядок складання звітів та інформування про події;

5) ролі та відповідальність підрозділів (працівників, адміністраторів) суб’єкта платіжного ринку за реалізацію політики управління конфігурацією.

36. Система захисту інформаційних систем, які використовуються для переказу коштів, щонайменше повинна забезпечувати автоматичну реєстрацію таких подій:

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

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

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

4) результатів виконання користувачем операцій з оброблення інформації, спроб несанкціонованих дій з інформацією;

5) подій, пов’язаних із зміною конфігураційних налаштувань компонентів інформаційних систем;

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

38. Відповідальні особи за забезпечення захисту інформації, інформаційної безпеки та кіберзахисту мають здійснювати регулярний перегляд і аналіз зареєстрованих подій інформаційної безпеки з метою виявлення незвичайної або підозрілої активності, складати звіти і вживати встановлені для цих випадків дії.

39. Засоби реєстрації подій інформаційної безпеки та записи про зареєстровані події мають бути захищені від модифікації та знищення користувачами, які не мають повноважень адміністратора.

40. Суб'єкт платіжного ринку зобов'язаний проінформувати Національний банк про такі події:

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

2) події, які класифікуються згідно з 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 інформаційних системах, що використовуються для переказу коштів.

XIII. Управління життєвим циклом системи захисту

41. Суб'єкт платіжного ринку зобов'язаний вживати заходи для забезпечення захисту інформації, інформаційної безпеки та кіберзахисту на всіх стадіях життєвого циклу системи захисту, що використовується для переказу коштів: при підготовці до експлуатації, при введенні в експлуатацію, в ході безпосередньої експлуатації і при знятті з експлуатації.

42. Суб'єкт платіжного ринку при формуванні вимог до системи захисту повинен враховувати вимоги до захисту інформації та кіберзахисту чинного законодавства та вимоги цього положення.

Ключовий суб'єкт платіжного ринку зобов'язаний самостійно формувати вимоги до системи захисту інформації за результатами:

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

2) аналізу можливих вразливостей інформаційних систем, а також програмно-апаратних засобів захисту інформації, серверного і мережевого обладнання;

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

43. Ключовий суб’єкт платіжного ринку повинен:

1) використовувати систему захисту інформації, що має технічну підтримку від розробників або створена і підтримується безпосередньо ключовим суб’єктом платіжного ринку;

2) провести функціональні випробування ПЗ, що забезпечує захист інформації, перед його впровадженням у дослідну чи промислову експлуатацію, та виконати перевірку вихідних текстів фахівцями, незалежними від розробників;

3) під час розробки, впровадження та експлуатації власного ПЗ, що використовується для захисту інформації, необхідно забезпечити усунення всіх відомих вразливостей.

Додаток 1
до Положення про захист інформації
та кіберзахист в платіжних системах
(підпункт 6 пункту 10 розділу III)

Вимоги до логінів та паролів

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

2. Зберігання та передавання паролів здійснюється в захищеному від НСД вигляді.

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

1) у випадку використання в якості одного з факторів 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 за забезпечення захисту інформації, інформаційної безпеки та кіберзахисту 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.

Додаток 2
до Положення про захист інформації
та кіберзахист в платіжних системах
(пункт 27 розділу VIII)

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 “Системи обробки інформації. Захист криптографічний. Алгоритми криптографічного перетворення”, затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495	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	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)	Не менше 160
4	Національний стандарт України ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, затверджений наказом Державного комітету України 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. Ґеш-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 “Інформаційна технологія. Криптографічний захист інформації. Функція ґешування”, 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 України ДСТУ 7564-2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”, затверджений наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431	Перевірка цілісності. Захист каналів	8 – 512
5	Message authentication code, MAC	Електронний підпис	Будь-яка довжина, передбачена цим алгоритмом