Типовий опис системи захисту інформації в правилах платіжної системи, платіжною організацією якої є резидент

Зразок правил	Пояснення до зразка правил
1. Загальні вимоги до захисту інформації Система захисту інформації в платіжній системі забезпечує захист інформації щодо переказу коштів на всіх етапах її формування, оброблення, передавання та зберігання відповідно до вимог законодавства України. Платіжна організація встановлює організаційні, технічні та технологічні вимоги до захисту інформації в платіжній системі та для суб'єктів переказу коштів. Учасники платіжної системи зобов'язані виконувати вимоги щодо захисту інформації, встановлені законодавством України та цими правилами. Про всі виявлені порушення вимог інформаційної безпеки в платіжній системі учасники платіжної системи зобов'язані повідомляти Платіжну організацію. У випадках наявності ознак вчинення злочину учасники також зобов'язані повідомляти про такі порушення правоохоронні органи. Головною метою впровадження в платіжній системі організаційних заходів та технічних засобів захисту інформації є: – захист інформації щодо електронних документів на переказ від несанкціонованого доступу, спотворення або знищення; – унеможливлення здійснення протиправних дій щодо інформації та інформаційних систем обслуговуючим персоналом. Головними об'єктами захисту у системі є: – електронні документи на переказ та їх архіви;	Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затверджене постановою Правління Національного банку України від 04.02.2014 № 43 (далі – Положення № 43) вимагає, щоб правила платіжної системи містили систему захисту інформації на всіх етапах функціонування платіжної системи. Для виконання такого опису слід окреслити межі застосовності вимог до системи захисту. Так, стаття 38 закону України «Про платіжні системи та переказ коштів в Україні» (далі – Закон) вимагає, щоб «Система захисту інформації забезпечувала безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання». До інформації щодо переказу коштів може бути віднесено: документи на переказ, інформаційні повідомлення, що прямо чи опосередковано стосуються переказів, інформація з обмеженим доступом щодо Платників та Отримувачів.

– інформаційні повідомлення між Платіжною організацією, розрахунковим банком, операторами послуг платіжної інфраструктури, учасниками платіжної системи та іншими суб'єктами переказу коштів; – інформація з обмеженим доступом, що зберігається в базах даних платіжної системи та резервних копіях; – інформація про платників та отримувачів переказів; – засоби оброблення та захисту інформації (програмно-технічні та криптографічні); – серверне та мережеве обладнання задіяне для переказу коштів; – криптографічні ключі, паролі та інша конфіденційна інформація, яка використовується для авторизації програмно-технічними засобами та користувачами.	
2. Організаційні, технічні та криптографічні заходи Учасники платіжної системи повинні передбачити в своїй організаційній структурі посади відповідальних працівників, до функціональних обов'язків яких входитиме управління інформаційною безпекою та адміністрування засобів захисту інформації. З метою запобігання порушення інформаційної безпеки в платіжній системі Платіжна організація здійснює такі організаційні заходи: 1) виявляє джерела загроз безпеці інформації та кібербезпеці та проводить оцінку потенційних можливостей зовнішніх та внутрішніх порушників; 2) проводить аналіз можливих вразливостей інформаційних систем, а також програмно-апаратних засобів захисту інформації, серверного і мережевого обладнання; 3) визначає можливі способи реалізації загроз інформаційній	Положення № 43 вимагає, щоб правила платіжної системи (далі – Правила) містили систему захисту інформації на всіх етапах функціонування платіжної системи. Захист інформації здійснюється за допомогою організаційних, інженерних, технічних та криптографічних заходів. Відповідно до пункту 38.4 Закону захист інформації забезпечується суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається із ряду заходів, зокрема, заходів персоналу суб'єкта переказу. Тому рекомендується вказати такі вимоги. Оскільки пункт 38.6 Закону встановлює, що розробка технологічних засобів криптографічного захисту здійснюється Платіжною організацією відповідної платіжної системи, її учасниками або іншою установою

безпеці; 4) оцінює можливі наслідки від виникнення загроз інформаційній безпеці, порушення окремих властивостей безпеки інформації (цілісність, доступність, конфіденційність), а також системи захисту інформації в цілому. За результатами цих заходів Платіжна організація формує зміни до вимог щодо інформаційної безпеки та кібербезпеки учасників платіжної системи. З метою забезпечення захисту інформації та запобігання ризикам інформаційної безпеки в платіжній системі, Платіжна організація платіжної системи, учасники платіжної системи, оператор послуг платіжної інфраструктури здійснюють такі технічні та криптографічні заходи: – застосування сертифікованих засобів криптографічного захисту для інформації, вимога щодо захисту якої встановлена законом; – використання удосконаленого або кваліфікованого електронного підпису на електронних документах на переказ; – керування розподілом прав доступу користувачів (Платіжної організації платіжної системи, учасників платіжної системи, оператора послуг платіжної інфраструктури, платників, отримувачів) до інформаційних систем, облік засобів доступу до них, персоніфікація здійснення дій користувачами, а також протоколювання цих дій; – впровадження парольних політик; – керування генерацією, обліком та поширенням ключової інформації; – використання захищених (шифрованих) каналів та протоколів під час передачі інформації; – застосування засобів захисту баз даних;	на їх замовлення, слід визначити хто саме в платіжній системі встановлює вимоги до побудови системи захисту та використання криптографічних засобів захисту інформації.

– здійснення антивірусного захисту на серверах, віртуальних машинах, робочих комп'ютерах працівників; – використання засобів діагностики та моніторингу для контролю цілісності баз даних, програмного забезпечення та системних файлів; – моніторинг мережевого трафіку з метою виявлення злочинних дій і спроб здійснення несанкціонованого доступу до програмно-апаратних компонентів; – фільтрація та обмеження мережевого трафіку по IP-адресам, протоколам, портам; – автоматична фіксація (протоколювання) всіх подій у програмно-апаратних засобах, а також виконання фінансових та службових операцій; – резервне копіювання системних компонентів, програмного забезпечення, баз даних та інформації, що створюється під час надання послуг з переказу коштів; – впровадження автоматичного моніторингу фінансових операцій та реагування на виявлені підозрілі операції та інші заходи.	
3. Внутрішні нормативні акти суб'єктів переказу коштів Платіжна організація платіжної системи розробляє рекомендації та нормативні документи щодо захисту інформації учасниками платіжних систем та здійснює контроль за наявністю у суб'єктів переказу таких внутрішніх нормативних документів щодо інформаційної безпеки: – політика інформаційної безпеки; – порядок дій обслуговуючого персоналу, відповідального за інформаційну безпеку, під час виникнення стихійних лих, техногенних катастроф, страйків, масових заворушень та інших	Положення № 43 вимагає, щоб правила платіжної системи містили опис системи захисту інформації на всіх етапах функціонування платіжної системи. Пункт 38.4 Закону вимагає, щоб захист інформації забезпечувався суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається з внутрішніх нормативних актів суб'єктів переказу, що регулюють порядок доступу та роботи з відповідною інформацією. Таким чином, Правила повинні встановлювати

обставин непереборної сили; – порядок проведення навчань обслуговуючого персоналу з питань інформаційної безпеки; – положення про використання криптографічних засобів захисту інформації та криптографічних ключів на всіх етапах життєвого циклу; – порядок обліку, зберігання, використання та знищення носіїв, що містять інформацію з обмеженим доступом; – вимоги до засобів захисту мережі для з'єднань з програмно-технічними комплексами самообслуговування (ПТКС) та пунктами надання фінансових послуг (ПНФП), а також до забезпечення функціонування вебсайту в демілітаризованій зоні; – опис ролей та їх функціональності для доступу до серверного обладнання та засобів захисту мережі; – перелік портів та застосунків учасника.	повний перелік своїх нормативних документів необхідних для забезпечення захисту інформації. Запропонований перелік є орієнтовним і залежить від переліку послуг, що надаються платіжною системою, топології її інформаційних ресурсів тощо.
4. Відповідальність за порушення правил інформаційної безпеки Відповідальні особи учасника платіжної системи несуть персональну відповідальність за порушення вимог інформаційної безпеки відповідно до чинного законодавства України. Платник зобов'язаний дотримуватися вимог платіжної системи щодо захисту інформації. У випадку недотримання цих вимог Платник зобов'язаний відшкодувати шкоду, заподіяну банку або іншій установі – учаснику платіжної системи, що його обслуговує. При цьому учасник платіжної системи, що обслуговує платника, звільняється від відповідальності перед платником за проведення переказу.	Відповідно до пункту 39.1 Закону суб'єкти переказу зобов'язані виконувати встановлені законодавством України та правилами платіжних систем вимоги щодо захисту інформації, яка обробляється за допомогою цих платіжних систем. Правила платіжних систем мають передбачати відповідальність за порушення цих вимог з урахуванням вимог законодавства України. Тому в Правилах потрібно прописати відповідну відповідальність. Пунктом 33.3 Закону встановлено, що Платник зобов'язаний відшкодувати шкоду, заподіяну банку або іншій установі – учаснику платіжної системи, що його обслуговує, внаслідок недотримання цим Платником вимог щодо захисту інформації і проведенням незаконних

	операцій з компонентами платіжних систем (платіжні інструменти, обладнання, програмне забезпечення тощо). При цьому банк або інша установа – учасник платіжної системи, що обслуговує платника, звільняється від відповідальності перед платником за проведення переказу. Враховуючи це, в Правилах необхідно прописати також і відповідальність за інформаційну безпеку Платників.
5. Заходи з охорони приміщень Все серверне та мережеве обладнання, задіяне для переказу коштів в платіжній системі, повинно знаходитись в приміщеннях дата-центрів та відповідати наступним вимогам: – обладнання розташовано в окремій серверній стійці, яка зачиняється та опечатується; – фізичний доступ до серверного та мережевого обладнання мають лише відповідальні за інформаційну безпеку особи; – в приміщеннях з обладнанням ведеться цілодобове відео-спостереження; – приміщення обладнане автоматизованою системою протипожежного захисту; – приміщення знаходиться під цілодобовою охороною; – серверне та мережеве обладнання забезпечене основним та резервним безперебійним живленням.	Положення № 43 вимагає, щоб правила платіжної системи містили опис системи захисту інформації на всіх етапах функціонування платіжної системи. Відповідно до пункту 38.4 Закону захист інформації забезпечується суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається, зокрема, із заходів охорони приміщень. Запропоновані заходи засновані на кращих практиках з охорони приміщень та можуть бути уточнені в залежності від побудови системи захисту платіжної системи та її структури.
6. Технічний захист інформації На програмно-технічному рівні захист інформації здійснюється за допомогою засобів захисту мережі. Ці засоби забезпечують захист: – серверного обладнання, що задіяне для переказу коштів в платіжній системі;	Положення № 43 вимагає, щоб правила платіжної системи містили опис системи захисту інформації на всіх етапах функціонування платіжної системи. Оскільки захист інформації поділяється на організаційний, інженерний, технічний та криптографічний, необхідно приділити увагу кожному з них, зокрема технічному

– внутрішніх мережевих сервісів; – робочих місць адміністраторів; – програмних застосунків на серверах та робочих місцях працівників. З метою запобігання порушень інформаційної безпеки та уникнення кіберінцидентів здійснюється такі заходи: – встановлюється чіткий розподіл прав доступу до засобів захисту мережі, серверів та застосунків; – всі технічні, службові та фінансові операції протоколюються шляхом ведення журналів реєстрації; – забезпечується можливість відновлення до робочого стану всіх мережевих засобів захисту інформації та серверного обладнання у випадку збоїв.	захисту інформації.
7. Засоби захисту мережі Для захисту зовнішнього периметра від мережевих атак, забезпечення контролю доступу та створення захищених з'єднань використовуються міжмережеві екрани. Платіжна організація платіжної системи використовує в якості міжмережевого екрану ЗАСІБ1 моделі А виробництва компанії КОМПАНІЯ1. Засіб має позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України № 02/02/02–2222 від 01.01.2018 р., копія якого надається у ДОДАТКУ1. Вимоги до умов експлуатації, наведені в Розділі 10 цього висновку, виконуються в повному обсязі. Учасники платіжної системи можуть використовувати для захисту своїх мереж інші міжмережеві екрани за умови наявності на них чинного позитивного експертного висновку Державної служби спеціального зв'язку та захисту інформації	Положення № 43 вимагає, щоб правила платіжної системи містили систему захисту інформації на всіх етапах функціонування платіжної системи, уключаючи технологію використання засобів захисту інформації. Пункт 38.4 Закону вимагає, щоб захист інформації забезпечувався суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи захисту, що складається, зокрема, з технічного обладнання відповідної платіжної системи. Оскільки відповідно до пункту 38.1 Закону система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання, а технічне обладнання є складовою системи захисту, Правила платіжної системи повинні містити опис цих засобів захисту.

України. Всі міжмережеві екрани, що використовуються в платіжній системі повинні відповідати наступним вимогам: міжмережевий екран працює лише із вказаним діапазоном IP-адрес та портів, усі інші запити повинні блокуватися; сегмент мережі, в якому розміщено сервери баз даних та демілітаризована зона з вебсервером, розділені за допомогою міжмережевого екрану; перегляд налаштувань міжмережевого екрану здійснюється не рідше одного разу на 3 місяці. Учасники платіжної системи при використанні міжмережевих екранів повинні забезпечити: – заборону використання бездротових мереж; – заборону прямого доступу із зовнішніх мереж до налаштувань міжмережевого екрану, баз даних, журналів подій; – за допомогою механізму переадресації здійснюється запобігання розкриттю внутрішніх IP-адрес; – після змін налаштувань конфігурації маршрутизатора здійснюється виконання тестування всіх варіантів зовнішніх з'єднань; – на міжмережевому екрані відключено всі протоколи та сервіси, що не використовуються для виконання поставлених перед міжмережевим екраном задач; – в мережі створено окремий сервер реєстрації подій міжмережевого екрану; – в міжмережевому екрані встановлено всі актуальні оновлення внутрішнього програмного забезпечення та перед запуском маршрутизатора здійснюється контроль цілісності внутрішнього програмного забезпечення.	Національний банк не здійснює експертизу технічних засобів захисту інформації, тому необхідно надавати підтверджуючі документи щодо надійності цих засобів видані компетентними органами. В Україні таким органом є Державна служба спеціального зв'язку та захисту інформації в Україні. В Правилах слід вказати такі засоби та надати копії відповідних експертних висновків. Зазвичай, такі висновки містять перелік вимог, за умов виконання яких забезпечується надійність захисту інформації. В Правилах можна вказати, що всі вимоги експертного висновку виконуються, або вказати перелік таких вимог. Правила можуть містити також додаткові вимоги.

8. Антивірусний захист За допомогою антивірусного програмного забезпечення здійснюється захист серверів, вебсерверів та робочих місць працівників Платіжної організації платіжної системи та учасників платіжної системи. Має використовуватись виключно ліцензійне антивірусне програмне забезпечення. Антивірусне програмне забезпечення повинно мати постійну технічну підтримку від розробників.	Положення № 43 вимагає, щоб правила платіжної системи містили систему захисту інформації на всіх етапах функціонування платіжної системи. Також пунктом 38.1 Закону передбачено, що система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання. Однією із складових такого захисту є використання антивірусного програмного забезпечення.
9. Криптографічні засоби захисту інформації В платіжній системі передбачається використання наступних криптографічних засобів захисту інформації: 1) ЗАСІБ1. Розробником є ТОВАРИСТВО1. Засіб має позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України № 01/01/01–1111 від 01.01.2019 р., копія якого надається у ДОДАТКУ1. Термін дії експертного висновку: до 31.12.2024 р. ЗАСІБ1 використовується для: – шифрування за АЛГОРИТМОМ1 з довжиною ключів ДОВЖИНА1, ДОВЖИНА2, ДОВЖИНА3 та АЛГОРИТМОМ2 з довжиною ключів ДОВЖИНА4, ДОВЖИНА5. – накладання електронного підпису за АЛГОРИТМОМ3 з довжиною ключів ДОВЖИНА6 - ДОВЖИНА7. 2) КРИПТОГРАФІЧНА_БІБЛІОТЕКА1. Розробником є ТОВАРИСТВО2. Засіб має позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України № 01/01/01–1111 від 01.01.2018 р., копія якого надається у ДОДАТКУ1. Термін дії експертного висновку до 31.12.2023 р. КРИПТОГРАФІЧНА_БІБЛІОТЕКА1	Положення № 43 вимагає, щоб правила платіжної системи містили опис системи захисту інформації на всіх етапах функціонування платіжної системи, уключаючи найменування алгоритмів і довжину ключів, паролів, технологію використання засобів захисту інформації, інформацію про розробника цих засобів. Тому в Правилах необхідно вказати всі засоби криптографічного захисту інформації та їх розробників, вказати, де саме ці засоби використовуються, описати криптографічні алгоритми, що можуть використовуватися в платіжній системі та довжини ключів. Довжини ключів можуть задаватися таким чином: «не менше…», «в діапазоні…» У випадку використання процедури формування сертифікатів відкритих ключів для удосконаленого електронного підпису, система захисту інформації включає в себе також і програмно-технічний комплекс, за допомогою якого буде виконуватися така сертифікація. У випадку пересилання відкритого ключа на сертифікацію система захисту інформації має включати в себе заходи по встановленню авторства цього відкритого ключа.

використовується для: –- обрахунку ґеш-функції за АЛГОРИТМОМ3 з довжиною ключів ДОВЖИНА8; – шифрування за АЛГОРИТМОМ4 з довжиною ключів ДОВЖИНА9, ДОВЖИНА10, ДОВЖИНА11 та АЛГОРИТМОМ5 з довжиною ключів ДОВЖИНА12, ДОВЖИНА13. – накладання електронного підпису за АЛГОРИТМОМ6 з довжиною ключів ДОВЖИНА14 - ДОВЖИНА15.	Слід взяти до уваги, що відповідно до пункту 38.2 Закону електронні документи на переказ, розрахункові документи під час їх передавання засобами телекомунікаційного зв'язку повинні бути зашифровані. Також пунктом 19.2 Закону встановлено, що електронні документи зберігаються на носіях інформації у формі, що дозволяє перевірити цілісність, достовірність та авторство електронних документів на цих носіях. Розділом IV Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 визначено, що для криптографічного захисту інформації, вимога щодо захисту якої встановлена законом, повинні використовуватися засоби, що мають чинний експертний висновок Держспецзв'язку (Державної служби спеціального зв'язку та захисту інформації України). Невиконання цієї вимоги є порушенням законодавства. Таким чином, до Правил необхідно надати копії чинних експертних висновків на криптографічні засоби захисту інформації, які використовуються для виконання норм Закону. При описі криптографічних засобів захисту інформації слід враховувати, що ці засоби можуть використовуватися з метою виконання також інших норм Закону, а саме: – пункт 38.4. Захист інформації забезпечується суб'єктами переказу коштів шляхом обов'язкового впровадження та використання відповідної системи

	захисту, що складається з програмно-апаратних засобів криптографічного захисту інформації, яка обробляється в платіжній системі; – пункт 38.5. Система захисту інформації повинна забезпечувати: неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання.
10. Система керування ключами Платіжна організація платіжної системи встановлює своїми внутрішніми документами вимоги до управління ключами, включаючи процедури їх генерації, використання та знищення як для забезпечення криптографічного захисту інформації в платіжній системі, так і для функціонування системи захисту. Зокрема використовуються наступні типи криптографічних ключів: 1) ПАРА КЛЮЧІВ1. Використовується для створення удосконаленого електронного підпису на електронні документи на переказ за АЛГОРИТМОМ3 з довжиною ключів ДОВЖИНА6. Особистий ключ генерується за допомогою криптографічного засобу захисту інформації ЗАСІБ1 та зберігається в ньому протягом всього періоду його використання. Доступ підписувача до ключа можливий лише після введення паролю. Відповідальність за збереження засобу накладання удосконаленого електронного підпису несе підписувач. Термін дії ключа не більше 1 року. Відкритий ключ визнається чинним шляхом підписання акту про взаємне визнання ключів.	Положення № 43 вимагає, щоб правила платіжної системи містили опис системи захисту інформації на всіх етапах функціонування платіжної системи, уключаючи систему керування ключами. Система керування ключами передбачає встановлення вимог до генерації, передачі, зберігання та обліку криптографічних ключів, а також до терміну їх життя і періодичності заміни.

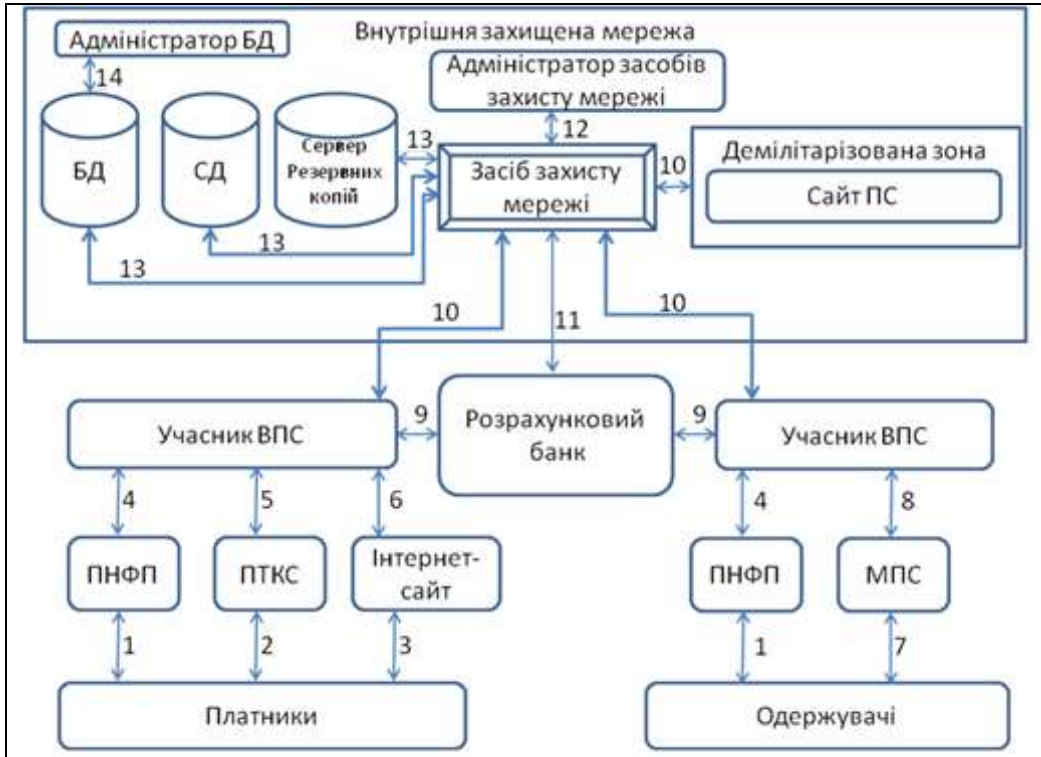
2) ПАРА КЛЮЧІВ2. Використовується для створення кваліфікованого електронного підпису на архіви електронних документів на переказ. Особистий ключ генерується за допомогою криптографічного засобу захисту інформації КРИПТОГРАФІЧНА БІБЛІОТЕКА1. Криптографічний алгоритм – АЛГОРИТМ6, довжина ключів ДОВЖИНА14 – ДОВЖИНА15. Видавцем кваліфікованого сертифікату відкритого ключа є ЮРИДИЧНА ОСОБА1. Зберігання особистого ключа відповідальними особами здійснюється на флеш-накопичувачах або зовнішніх жорстких дисках та зовнішніх твердотільних накопичувачах за умови шифрування цих ключів з використанням криптографічних алгоритмів АЛГОРИТМ7, ключ якого формується з паролю відповідальної особи; Термін дії ключа визначається кваліфікованим надавачем електронних довірчих послуг відповідно до законодавства України. У випадку втрати чи компрометації особистого ключа відповідальний за цей ключ повідомляє Платіжну організацію платіжної системи та потенційних одержувачів електронних документів, на який накладено електронний підпис з використанням цього ключа, про те, що цей ключ є недійсним. Після одержання такого повідомлення електронні документи, на які накладено електронний підпис з використанням цього ключа, вважаються недостовірними.	
11. Вимоги до паролів Автентифікація відповідальних осіб до власних інформаційних систем або інформаційних систем процесингового центру здійснюється з використанням логіну та паролю. Паролі поділяються на тимчасові та довготривалі. Тимчасові паролі встановлюються адміністратором	Положення № 43 вимагає, щоб правила платіжної системи містили: технологію обміну інформацією в платіжній системі…, уключаючи порядок доступу; систему захисту інформації на всіх етапах функціонування платіжної системи, уключаючи… довжину паролів.

інформаційних систем під час реєстрації відповідальної особи або втрати чи компрометації попереднього паролю. Після першої автентифікації відповідальної особи тимчасовий пароль підлягає заміні відповідальною особою на довготривалий. Довготривалі паролі підлягають заміні не рідше одного разу на 60 календарних днів. Прострочений пароль не може бути змінений віддалено. На серверах паролі повинні зберігатися у вигляді ґеш-функції від паролю з додаванням «солі». «Сіль» надсилається відповідальній особі під час процедури автентифікації. Паролі передаються по мережі виключно в захищеному вигляді. 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). У випадку введення неправильного паролю п’ять разів поспіль логін відповідальної особи блокується. Для розблокування логіну відповідальна особа повинна звернутися до адміністратора інформаційної системи.	Пункт 38.5 Закону встановлює, що система захисту інформації повинна забезпечувати конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі та забезпечення постійного та безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором. Такий договір може бути укладено, наприклад, між учасниками платіжної системи та Платіжною організацією. Правила повинні містити вимоги до паролів, порядок їх створення та використання, який забезпечує виконання вимог Закону.
12. Захист інформаційних систем Інформаційні системи, що здійснюють обробку даних платіжної системи, які є об’єктом захисту, розміщуються в процесинговому центрі платіжної організації та в учасників платіжної системи. Програмне забезпечення інформаційних систем розробляється та експлуатується з урахуванням вимог інформаційної безпеки та кібербезпеки, встановлених законодавством України, нормативно-правовими актами Національного банку України та кращими світовими	Положення № 43 вимагає, щоб правила платіжної системи містили технологію обміну інформацією в платіжній системі, уключаючи порядок обміну інформацією з віддаленими робочими місцями приймання/виплати переказів (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування тощо). Пункт 38.5 Закону встановлює, що система захисту інформації повинна забезпечувати: 1) цілісність інформації, що передається в платіжній

практиками. Вбудована в програмне забезпечення система захисту забезпечує неможливість обробки інформації в обхід цієї системи захисту та її несанкціоноване відключення. Система захисту інформаційних систем забезпечує: – цілісність інформації, що отримує та обробляє інформаційна система; – конфіденційність інформації під час її обробки, передавання та зберігання; – неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання; – забезпечення постійного та безперешкодного доступу до інформаційних систем особам, які мають на це право або повноваження відповідно до законодавства України, а також встановлених Договорами (…); – користувачі інформаційних систем не мають прямого доступу до баз даних з інформацією, що є об'єктом захисту; – відміна внесення електронного документу на переказ реєструється, як окрема операція, а попередні записи в базах даних не видаляються; – інформаційні системи ведуть журнали критичних подій (зміна паролю, створення документу на переказ, зміна інформації щодо точок надання послуг, зміна користувачів, зміна тарифів та лімітів) та спроб входу користувачів до інформаційних систем; – журнал критичних подій захищається за допомогою накладання електронного підпису на підпис більш ранньої версії журналу, об'єднаного з ґеш-функцією нового запису; – перед початком роботи інформаційної системи системою	системі, та компонентів платіжної системи; 2) конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі. Пункт 39.2 Закону вимагає, що при проведенні переказу його суб'єкти мають здійснювати в межах своїх повноважень захист відповідної інформації від: 1) несанкціонованого доступу до інформації – доступу до інформації щодо переказу, що є банківською таємницею або є іншою інформацією з обмеженим доступом, осіб, які не мають на це прав або повноважень, визначених законодавством України, а також якщо це не встановлено договором; 2) несанкціонованих змін інформації – внесення змін або часткового чи повного знищення інформації щодо переказу особами, які не мають на це права або повноважень, визначених законодавством України, а також встановлених договором; 3) несанкціонованих операцій з компонентами платіжних систем – використання або внесення змін до компонентів платіжної системи протягом її функціонування особами, які не мають на це права або повноважень, визначених законодавством України, а також встановлених договором. Як правило, виконання цих вимог забезпечують інформаційні системи, що здійснюють обробку документів на переказ та інших інформаційних повідомлень та забезпечують розмежування прав доступу для різних типів користувачів. Тому в правилах варто надати опис вимог до захисту інформації цих інформаційних систем.

захисту здійснюється перевірка цілісності баз даних та програмного забезпечення. В інформаційній системі можливе створення облікових записів користувачів з такими функціональними ролями: адміністратор інформаційної системи, адміністратор бази даних, користувачі, користувачі служби підтримки, тощо. Адміністратор інформаційної системи має доступ до журналу критичних подій в режимі читання та може здійснювати аналіз цих журналів та формування звітів про виконані операції, про невдалі спроби входу користувачів, а також має доступ виключно до створення та модифікації облікових записів інших користувачів та до налаштувань інформаційної системи. Адміністратор баз даних здійснює супровід баз даних, включаючи створення резервних копій та відновлення бази даних у випадках збоїв. Користувачі інформаційної системи мають право здійснювати операції з переказу коштів. Користувачі служби підтримки мають можливість одержувати інформацію про стан системи, переглядати інформацію в базі даних, змінювати довідники та інші допоміжні дані. Розробники інформаційної системи здійснюють розробку і тестування виключно в тестовому середовищі та не мають доступу до діючої інформаційної системи. Для захисту журналів шляхом накладання електронного підпису використовується КРИПТОГРАФІЧНА_БІБЛІОТЕКА1 з використанням АЛГОРИТМУ6 з довжиною ключів ДОВЖИНА14. Захист журналів операційної системи, гіпервізора та бази даних БАЗА_SQL здійснюється за допомогою власних засобів цієї операційної системи, гіпервізора або бази даних.	

13. Автентифікація Автентифікація доступу до інформаційних систем користувачів здійснюється з використанням унікального логіну та паролю. Автентифікація відповідальних осіб ПНФП та адміністраторів інформаційних систем здійснюється з використанням багатофакторної автентифікації, яка полягає в надсиланні системою захисту інформаційної системи на мобільний телефон користувача sms-повідомлення з паролем, який користувач повинен надіслати до інформаційної системи під час автентифікації. Створення нових облікових записів, їх модифікація та видалення належать до компетенції призначених платіжною організацією або керівництвом учасника адміністраторами інформаційної безпеки. Після проходження автентифікації користувач інформаційної системи може користуватись системою протягом робочого дня. У випадку бездіяльності користувача протягом 10 хвилин сесія обміну інформаційними повідомленнями з інформаційною системою завершується. Для подальшої роботи користувач повинен виконати процедуру автентифікації повторно.	Положення № 43 вимагає щоб правила платіжної системи містили технологію обміну інформацією в платіжній системі, уключаючи порядок доступу. Заходом із забезпечення порядку доступу віддалених користувачів є автентифікація.
14. Загальна схема інформаційних потоків з описом захисту інформації на кожній її ланці	Положення № 43 вимагає щоб правила платіжної системи містили схему обміну інформацією, яка використовується в платіжній системі та систему захисту інформації на всіх етапах функціонування платіжної системи, уключаючи найменування алгоритмів і довжину ключів, паролів, технологію використання засобів захисту інформації, інформацію про розробника цих засобів, систему керування ключами. Найпростіше виконати ці вимоги шляхом



Ланка №1. Платник особисто звертається до ПНФП та після внесення коштів власноручно пише заяву на переказ коштів, засвідчуючи її особистим підписом.

Ланка №2. Платник за допомогою ПТКС створює електронний документ на переказ коштів. Електронний підпис на електронний документ створюється за допомогою криптографічної бібліотеки КРИПТОГРАФІЧНА БІБЛІОТЕКА1 (інформацію щодо якої наведено в пункті 9) та криптографічний ключ КЛЮЧ1.

відображення загальної схеми обміну інформаційними повідомленнями (без схеми обміну грошовими коштами), пронумерувати ланки обміну інформаційними повідомленнями та надати опис захисту інформації на кожній ланці. Такий опис повинен вказувати технології захисту інформаційного обміну на відповідній ланці. При цьому повинно забезпечуватись виконання таких пунктів Закону:

– 38.1. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання.

– 38.2. Електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням електронних платіжних засобів, що містять банківську таємницю, під час їх передавання засобами телекомунікаційного зв’язку повинні бути зашифровані згідно з вимогами відповідної платіжної системи, а за їх відсутності – відповідно до вимог законів України та нормативно-правових актів Національного банку України.

Ланка №3. Платник створює захищене з’єднання з Інтернет-сайтом, використовуючи протокол HTTPS. Параметри протоколу HTTPS: алгоритм ґешування SHA1, ключ шифрування RSA з довжиною 2048 біт, видавець сертифікату КОМПАНІЯ1. Захищене з’єднання забезпечується використанням криптографічного протоколу TLS 1.2 (Transport Layer Security). З метою узгодження спільного ключа використовується криптографічний алгоритм АЛГОРИТМ з довжиною ключів ДОВЖИНА_КЛЮЧА та ґешфункція ГЕШФУНКЦІЯ з довжиною блоку ДОВЖИНА. Для обміну інформаційними повідомленнями використовується спільний ключ симетричного алгоритму шифрування АЛГОРИТМ з довжиною ключа ДОВЖИНА. Сертифікат сайту засвідчується одним з таких центрів сертифікації : ЦЕНТР1, ЦЕНТР2, ЦЕНТР3. Ланка №4. Відповідальна особа ПНФП для обміну інформаційними повідомленнями створює захищене з’єднання з програмно-технічним комплексом учасника ВПС. Захищене з’єднання створюється за допомогою каналу VPN. Канал створюється з використанням засобу захисту мережі ЗАСІБ, що має позитивний експертний висновок Державної служби спеціального зв’язку та захисту інформації України № 01/01/01–1111 від 01.01.2019 р., копія якого надається у ДОДАТКУ1. Для створення каналу використовується набір протоколів IPSEC зі спільним ключем з довжиною ДОВЖИНА та криптографічним алгоритмом АЛГОРИТМ. Для обміну інформаційними повідомленнями на цій ланці відповідальна особа ПНФП проходить процедуру автентифікації в програмно-апаратному комплексі учасника. Ця процедура може проводитися одним з	

наступних способів. Спосіб1: Відповідальна особа після встановлення захищеного з'єднання вводить свій логін та пароль. Спосіб2: Відповідальна особа вводить номер свого мобільного телефону, на який приходить sms-повідомлення з кодом підтвердження, який також необхідно ввести. Всі інформаційні повідомлення щодо переказу коштів повинні мати електронний підпис відповідальної особи. В якості такого підпису може використовуватися кваліфікований електронний підпис або удосконалений електронний підпис, опис якого надано в пункті 1.8. Ланка №5. Захист зв'язку між ПТКС та учасником встановлюється за допомогою протоколу HTTPS. Параметри протоколу відповідають вказаним при описі ланки №3. Всі електронні документи на переказ, що створюються за допомогою ПТКС, повинні мати електронний підпис, що формується за допомогою КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ1 з використанням криптографічного алгоритму АЛГОРИТМ6 з довжиною ключів ДОВЖИНА14 або ДОВЖИНА15. Цей електронний підпис перевіряється в процесинговому центрі учасника. Ланка №6. Інтернет-сайт учасника повинен знаходитися в демілітаризованій зоні учасника та бути захищеним від мережі загального користування та внутрішньої мережі учасника за допомогою засобу захисту мережі, що погоджений з платіжною організацією платіжної системи. Обмін інформацією на цій ланці захищається цим засобом захисту мережі.	

Ланка №7. Обмін інформацією на цій ланці забезпечується відповідно до вимог міжнародної карткової платіжної системи КПС1. Ланка №8. Обмін інформацією на цій ланці забезпечується відповідно до вимог міжнародної карткової платіжної системи КПС1. Ланка №9. Обмін інформаційними повідомленнями щодо переказу коштів учасниками здійснюється за допомогою системи Клієнт-банк. Захист інформації на цій ланці та порядок автентифікації здійснюється відповідно до вимог банку. Автентифікація відповідальної особи здійснюється за допомогою двофакторної автентифікації (за паролем та кодом, що генерується за допомогою OTP (One Time Password), виданого банком). Електронні документи, що передаються до банку засвідчуються кваліфікованим електронним підписом. Захищене з'єднання забезпечується використанням криптографічного протоколу TLS версії не нижче 1.2. Ланка №10. Захист зв'язку між учасником та вебінтерфейсами процесингового центру платіжної системи встановлюється за допомогою протоколу HTTPS. Параметри протоколу відповідають вказаним в описі ланки №3. Всі інформаційні повідомлення повинні мати електронний підпис, вимоги до якого встановлено в описі ланок №4 та №5. Захист від несанкціонованого доступу забезпечується за допомогою засобу захисту мережі ЗАСІБ1, вимоги до якого наведено в розділі 1.6.	

Ланка №11. Захист інформації на цій ланці забезпечується відповідно до вимог системи Клієнт-банк розрахункового банку. Захист від несанкціонованого доступу забезпечується за допомогою засобу захисту мережі ЗАСІБ1, вимоги до якого наведено в розділі 1.6. Ланка №12. Адміністратор засобу захисту мережі здійснює адміністрування на цій ланці виключно через консольний порт в межах контрольованої зони. Ланка №13. Обмін інформацією в межах захищеного сегменту внутрішньої мережі здійснюється з використанням захисту мережі ЗАСІБ1, вимоги до якого наведено в розділі 1.6. Ланка №14. Адміністратор баз даних здійснює адміністрування безпосередньо на сервері баз даних, знаходячись в межах контрольованої зони.	
15. Порядок обміну інформацією в платіжній системі Платник ініціює операцію з переказу коштів одним з таких способів: – шляхом звернення до ПНФП, де за допомогою відповідальної особи заповнює реквізити платежу, після цього відповідальна особа накладає свій удосконалений електронний підпис на створений електронний документ на переказ; – шляхом вибору на ПТКС відповідної форми для внесення реквізитів платежу та, заповнюючи їх, ініціює створення електронного документу на переказ, а засобами КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ1 програмним забезпеченням ПТКС здійснюється створення електронного	Положення № 43 вимагає щоб правила платіжної системи містили технологію обміну інформацією в платіжній системі, уключаючи порядок обміну інформацією з віддаленими робочими місцями приймання/виплати переказів (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування тощо), а також технологію обміну інформацією між платіжною системою і системою автоматизації банку для обліку переказів коштів (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування тощо). Тому або безпосередньо при описі захисту

підпису на електронний документ; – платник шляхом заповнення реквізитів електронного документу на переказ на вебсайті учасника платіжної системи створює електронний документ на переказ та накладає свій кваліфікований електронний підпис на цей документ. Створений електронний документ на переказ разом з електронним підписом відправляється до процесингового центру учасника, де йому присвоюється унікальний код операції. У випадку використання платником ПТКС або вебсайту документ на переказ відправляється через автоматично створене захищене з'єднання. У випадку створення електронного документу на переказ працівником ПНФП цей працівник ініціює створення захищеного з'єднання з процесинговим центром учасника та власноручно відправляє створений електронний документ на переказ. Після успішної перевірки електронного підпису на електронному документі підтвердження успішності створення електронного документу та унікальний код операції передається платнику. Платник зручним способом повідомляє цей код Одержувачу. Процесинговий центр учасника через захищене з'єднання передає інформацію щодо одержаних ним документів на переказ до процесингового центру платіжної системи, де ця інформація зберігається в базі даних переказів платіжної системи. Одержувач може отримати кошти двома шляхами: звернутись до ПНФП учасника або отримати переказані кошти на свій рахунок. У випадку переказу коштів на рахунок банк – учасник платіжної системи здійснює зарахування коштів на банківський рахунок Одержувача за вказаними Платником реквізитами.	інформації на кожній ланці інформаційних повідомлень, або в окремому розділі необхідно надати опис саме технології обміну захищеною інформацією. Найбільшу увагу слід приділити порядку накладання електронного підпису на електронний документ та його перевірці, оскільки відповідно до статті 18 Закону електронний підпис є обов'язковим реквізитом електронного документа на переказ, а електронний документ на переказ, що не засвідчений електронним підписом, не приймається до виконання. Учасник платіжної системи має передбачити під час приймання електронних документів на переказ процедуру перевірки електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документа на переказ.

У випадку отримання Одержувачем коштів в ПНФП він звертається до оператора ПНФП та повідомляє унікальний номер переказу та інші реквізити переказу. Оператор ініціює встановлення захищеного з'єднання з процесинговим центром учасника для перевірки дійсності переказу. У випадку, якщо переказ здійснюється в межах одного учасника, процесинговий центр учасника надає підтвердження щодо достовірності переказу і оператор здійснює виплату переказу. У випадку, якщо переказ здійснюється між різними учасниками, процесинговий центр учасника встановлює з'єднання з процесинговим центром платіжної системи та надсилає запит для перевірки достовірності переказу. У випадку, якщо переказ достовірний, повідомлення про це надсилається на процесинговий центр учасника, а від нього на ПНФП. Після успішного зарахування переказу на рахунок або виплати в ПНФП інформація про завершення операції надсилається через процесинговий центр учасника до процесингового центру платіжної системи. З моменту одержання такого повідомлення переказ вважається виконаним. В кінці операційного дня за результатами виконаних операцій процесинговий центр системи розраховує за цей день нетто-позиції для кожного учасника платіжної системи. Після встановлення захищеного з'єднання з розрахунковим банком процесинговий центр системи через систему Клієнт-банк створює та надсилає відповідні платіжні доручення для виконання розрахунків між учасниками. Опис захисту інформації на цій ланці (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування) надано в пункті 14 Правил.	

16. Захист архівів електронних документів Електронні документи на переказ зберігаються в базі даних процесингового центру платіжної системи разом зі своїми електронними підписами. Інформаційні системи надають можливість за потреби під час перегляду електронного документу виконати перевірку підпису створеного для цього документу. Кожної доби з 0:00 до 0:30 здійснюється створення резервної копії баз даних електронних документів. Для резервної копії баз даних адміністратор баз даних створює кваліфікований електронний підпис за допомогою ЗАСОБУ1 з використанням криптографічного алгоритму АЛГОРИТМ3 з довжиною ключів не менше, ніж ДОВЖИНА6. Електронний підпис зберігається разом з базою даних. Щомісяця резервна копія баз даних записується на оптичний диск. Під час копіювання перевіряється цілісність, достовірність та авторство даних в резервній копії.	Положення № 43 вимагає, щоб правила платіжної системи містили систему захисту інформації на всіх етапах функціонування платіжної системи. Пункт 38.1 Закону встановлює, що система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі та зберігання. Одним з таких етапів, що потребує окремої уваги, є саме зберігання інформації. Пункт 19.2 Закону встановлює, що електронні документи зберігаються на носіях інформації у формі, що дозволяє перевірити цілісність, достовірність та авторство електронних документів на цих носіях, а копіювання електронних документів з метою їх подальшого зберігання має здійснюватися згідно з існуючим в установах порядком обліку та копіювання документів. При копіюванні електронного документа з носія інформації обов’язково має бути виконана перевірка цілісності, достовірності та авторства даних на цьому носії. Тому в цьому розділі пропонується вказати, яким чином в платіжній системі при збереженні інформації буде здійснюватися перевірка цілісності, достовірності та авторства електронних документів та даних.