ЗАТВЕРДЖЕНО
Рішенням Правління
ПАТ «НДУ»
від 20.09.2013 № 1/6

Положення
про інформаційно-телекомунікаційну систему обробки інформації Центрального депозитарію цінних паперів

(Положення про СОІ)

1. Загальні положення

1.1. Це Положення визначає організацію системи обробки і захисту інформації, перелік, опис та порядок використання компонентів інформаційно-телекомунікаційної системи обробки інформації (далі – СОІ) Публічного акціонерного товариства «Національний депозитарій України» (далі – Центральний депозитарій) у правовідносинах, що виникають під час здійснення ним професійної депозитарної діяльності Центрального депозитарію цінних паперів, а також вимоги до компонентів СОІ суб'єктів цих правовідносин.

1.2. Положення розроблене відповідно до Законів України «Про депозитарну систему України», «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг», Положення про провадження депозитарної діяльності, затвердженого рішенням Національної комісії з цінних паперів та фондового ринку (далі – Комісія) № 735 від 23.04.2013, а також Вимог до програмних продуктів на фондовому ринку, затверджених рішенням Комісії № 349 від 16.07.2003.

1.3. Вимоги цього Положення поширюється на Центральний депозитарій та таких учасників депозитарної системи України у разі набуття ними статусу учасника СОІ відповідно до вимог цього Положення:

- депозитарні установи;
- емітенти цінних паперів.

1.4. Учасники депозитарної системи України, перелічені у п.1.3 цього Положення, набувають статусу учасника СОІ після підписання з Центральним депозитарієм відповідного договору та, якщо інше не встановлено договором, – акту функціональної та технічної готовності до роботи в СОІ, який свідчить про виконання учасником депозитарної системи України вимог щодо програмного та технічного забезпечення, вимог із захисту інформації системи депозитарного обліку цінних паперів.

1.5. Центральний депозитарій організує та забезпечує функціонування СОІ.

2. Терміни, їх визначення та скорочення

2.1. У цьому Положенні вживаються такі терміни та скорочення:

- автоматизований режим обробки – процес обробки інформації (даних), що здійснюється програмним забезпеченням інформаційно-телекомунікаційної системи за участю користувача.

- автоматичний режим обробки – процес обробки інформації (даних), що здійснюється виключно програмним забезпеченням інформаційно-телекомунікаційної системи без участі користувача;
- вузли обробки даних учасника СОІ (ВОД) – сукупність організаційно-технологічних заходів, програмних та технічних засобів, призначених для обробки даних системи депозитарного обліку та інших даних у процесі здійснення діяльності учасника СОІ в рамках депозитарної системи України;
- електронне розпорядження – електронний документ визначеного формату та реквізитного складу, що ініціює виконання певної депозитарної операції;
- електронний цифровий підпис (ЕЦП) – дані, отримані за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати особу, що накладає електронний цифровий підпис;
- криптографічний захист інформації – (КЗІ) – захист інформації, яка передається між учасниками СОІ, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності та авторства;
- система керування базами даних (СКБД) – комп'ютерна програма чи комплекс програм, що забезпечує користувачам можливість створення, збереження, оновлення, пошук інформації та контролю доступу в базах даних;
- система обробки інформації (СОІ) – інформаційно-телекомунікаційна система, що використовується Центральним депозитарієм та іншими учасниками депозитарної системи України в їхніх правовідносинах в рамках депозитарної системи України;
- система обробки інформації (СОІ) – сукупність системного, прикладного програмного забезпечення систем передачі і обробки даних, комплексу технічних засобів та комплексу організаційних заходів, спрямованих на забезпечення здійснення електронних розрахунків за цінними паперами;
- система передачі даних (СПД) – модеми, маршрутизатори, ущільнювачі каналів, комутовані та виділені канали передачі даних;
- учасник СОІ – статус, якого набуває учасник депозитарної системи України відповідно до вимог цього Положення;
- центр сертифікації ключів – функціонально визначений підрозділ Центрального депозитарію, що забезпечує надання Центральним депозитарієм визначених законодавством послуг електронного цифрового підпису та забезпечує захист інформації з обмеженим доступом, що циркулює в СОІ, від порушення її конфіденційності та цілісності;
- інші терміни вживаються у значеннях, наведених у законодавстві.

3. Структура СОІ

3.1. Структура СОІ має дворівневу ієрархічну структуру (Центральний депозитарій та інші учасники СОІ) та складається з таких елементів:

- вузол обробки даних Центрального депозитарію;
- вузли обробки даних учасників СОІ;
- система передачі даних.

3.2. СОІ являє собою інформаційно-телекомунікаційну систему з такими основними видами забезпечення:

- інформаційне – сукупність інформаційних ресурсів, що обробляються на ВОД, засоби їх організації та реалізації;
- математичне та програмне – сукупність методів, моделей та алгоритмів обробки інформації, а також програм, правил та процедур, призначених для обробки інформації;
- лінгвістичне – мовні засоби опису та маніпулювання даними;
- технічне – сукупність технічних та телекомунікаційних засобів;
- організаційне – сукупність документів, що визначають організаційну структуру ВОД, права та обов'язки користувачів та персоналу;
- методичне – сукупність документів, що описують технологію функціонування ВОД, методи вибору та застосування користувачами технологічних прийомів під час обробки інформації.

3.3. Захист інформації, що циркулює в СОІ від загроз порушення конфіденційності, цілісності та доступності, здійснюється із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

3.4. Окремим компонентом комплексної системи захисту інформації СОІ, що входить до складу ВОД Центрального депозитарію, є акредитований центр сертифікації ключів (далі – АЦСК), який використовується для надання учасникам депозитарної системи України, зокрема, учасникам СОІ, послуг електронного цифрового підпису, а також для захисту інформації, що циркулює в СОІ, від несанкціонованого доступу.

4. Функції СОІ

4.1. СОІ забезпечує виконання депозитарних (адміністративних, облікових, інформаційних) операцій в автоматичному чи автоматизованому режимі у взаємодії Центрального депозитарію з іншими учасниками СОІ межах здійснення ними діяльності в рамках депозитарної системи України.

4.2. Для цього прикладне програмне забезпечення (далі – ППЗ) СОІ, зокрема, реалізує такі основні функції:

- виконання депозитарних операцій на рівні Центрального депозитарію та депозитарної установи;

- захищений обмін даними між Центральним депозитарієм та іншими учасниками СОІ;
- резервування програмних і технічних засобів, а також інформаційних ресурсів;
- захист інформації з обмеженим доступом, що міститься у системі депозитарного обліку;
- резервне копіювання та відновлення даних.

4.3. Функції СОІ реалізуються за рахунок вбудованих в ППЗ алгоритмів обігу (створення, оброблення, відправлення, передавання, одержання) електронних документів.

5. Порядок використання програмного забезпечення

5.1. Програмне забезпечення СОІ поділяється на:

5.1.1. Системне програмне забезпечення (операційні системи, системи керування базами даних, офісне).

5.1.2. Прикладне програмне забезпечення (ППЗ), що призначене для автоматизації процесів діяльності учасників СОІ як учасників депозитарної системи України, а також для забезпечення інформаційного обміну між ними (Модуль Центрального депозитарію, Модуль депозитарної установи, засоби захищеного обміну даними тощо).

5.1.3. Загальне програмне забезпечення (антивіруси, архіватори, засоби перегляду файлів різних форматів тощо).

5.2. Системне та загальне програмне забезпечення повинно бути отримано учасником СОІ або від Центрального депозитарію, або безпосередньо від виробника (дистриб'ютора) такого програмного забезпечення із дотриманням учасником СОІ ліцензійних умов використання такого програмного забезпечення. Використання конкретного загального програмного забезпечення повинно бути погоджене з Центральним депозитарієм за письмовим запитом Учасника СОІ.

5.3. ППЗ СОІ повинно отримуватись учасником СОІ виключно від Центрального депозитарію та використовуватись за таких умов та обмежень:

5.3.1. ППЗ СОІ є пропріетарним програмним забезпеченням Центрального депозитарію. Виключні майнові права інтелектуальної власності на ППЗ СОІ належать Центральному депозитарію.

5.3.2. ППЗ СОІ розповсюджується за ліцензією типу Royalty-free binaries («Freeware», Безкоштовно). Центральний депозитарій має право стягувати плату за технічне супроводження такого програмного забезпечення.

5.3.3. ППЗ СОІ повинно використовуватись учасником СОІ виключно для реалізації своїх прав та обов'язків учасника депозитарної системи України.

5.3.4. Учасник СОІ має право використовувати ППЗ СОІ протягом строку дії відповідного договору з Центральним депозитарієм.

5.3.5. Учасник СОІ не має право передавати право використання отриманого ППЗ СОІ будь-яким іншим особам.

5.3.6. Учаснику СОІ заборонено вчиняти з ППЗ СОІ такі дії: особисто та дозволяти будь-яким іншим особам копіювати, продавати, видавати ліцензії, поширювати, передавати, змінювати, адаптувати, здійснювати реверсний інжиніринг, перекладати, створювати похідні роботи, декомпілювати, розгруповувати або намагатися отримувати початковий код ППЗ СОІ в інший спосіб, вдаватися до будь-яких дій, щоб обійти, знищити захист або правила використання даних, що обробляються за допомогою ППЗ СОІ

5.3.7. Учаснику СОІ заборонено вчиняти такі дії: особисто та дозволяти будь-яким іншим особам використовувати ППЗ СОІ для отримання доступу, копіювання, передавання, повторного кодування або повторного передавання даних, що обробляються за допомогою ППЗ СОІ, з порушенням законодавства або прав третіх осіб.

5.3.8. Учаснику СОІ заборонено вчиняти такі дії: особисто та дозволяти будь-яким третім особам отримувати доступ до даних, переглядати, копіювати, поширювати дані, аналізувати вміст та структуру даних, змінювати або використовувати в інший спосіб дані, що обробляються за допомогою ППЗ СОІ, за допомогою інших програмних засобів окрім ППЗ СОІ.

5.4. Центральний депозитарій не несе відповідальності за коректність роботи ППЗ СОІ у разі невиконання учасником СОІ умов, визначених цим Положенням.

5.5. Центральний депозитарій має право стягувати плату за відновлення працездатності ППЗ СОІ у разі порушення учасником СОІ вимог його використання. Відновлення інформації здійснюється з урахуванням вимог, передбачених законодавством, за письмовим зверненням учасника СОІ, засвідченим підписом керівника та печаткою юридичної особи. Центральний депозитарій має право відмовити учаснику СОІ у відновленні працездатності ППЗ СОІ у випадку порушення цілісності інформації, що обробляється в СОІ, а також у випадку втрат, крадіжок, несанкціонованого знищення, викривлення, підроблення цієї інформації, що сталися з вини учасника СОІ. Відновлення працездатності ППЗ СОІ повинне виконуватись робочою групою, що створюється з числа співробітників Центрального депозитарію та учасника СОІ. За необхідністю, до

робочої групи можуть бути залучені представники розробника ППЗ СОІ.

5.6. Центральний депозитарій не несе відповідальності за шкоду, завдану учаснику СОІ неналежною роботою ППЗ СОІ у разі, якщо така робота була викликана деструктивним впливом стороннього програмного забезпечення або невиконанням учасником СОІ вимог встановленого цим Положенням порядку використання програмного забезпечення, ліцензійних умов щодо використання стороннього програмного забезпечення (у т.ч. використання неліцензійного програмного забезпечення).

6. Взаємодія Центрального депозитарію та депозитарної установи

6.1. Для організації інформаційного обміну з Центральним депозитарієм депозитарна установа повинна:

6.1.1. Підписати з Центральним депозитарієм депозитарний договір.

6.1.2. Відкрити в Центральному депозитарії рахунок у цінних паперах.

6.1.3. Надати заяву про приєднання до Умов договору про надання послуг електронного цифрового підпису Акредитованим центром сертифікації ключів Публічного акціонерного товариства «Національний депозитарій України».

6.1.4. Отримати засоби електронного цифрового підпису від Акредитованого центру сертифікації ключів НДУ. Сертифікат відкритого ключа електронного цифрового підпису та сам ключ повинні належати виключно особі, яка має право підпису відповідних документів в паперовому вигляді (розпорядник рахунку).

6.1.5. Отримати від Центрального депозитарію програмні засоби Модулю депозитарної установи, встановити та налагодити їх.

6.1.6. Встановити з’єднання з ВОД Центрального депозитарію та здійснити оновлення програмного та лінгвістичного забезпечення ВОД депозитарної установи.

6.1.7. Підписати Акт функціональної та технічної готовності до роботи в СОІ, який формується для підписання депозитарною установою одразу ж після здійснення першого успішного сеансу з ВОД Центрального депозитарію з обміну даними системи депозитарного обліку.

6.2. Функціонування СОІ відбувається в режимі послідовного відкриття і закриття операційних днів.

6.3. Депозитарна установа повинна забезпечити функціонування власного ВОД СОІ кожного операційного дня Центрального депозитарію, суворо дотримуючись відповідності дати поточного операційного дня депозитарної

установи з датою поточного операційного дня Центрального депозитарію.

6.4. Операційний день депозитарної установи повинен відкриватись кожного операційного дня Центрального депозитарію. Операційний день депозитарної установи повинен закриватись не раніше часу закриття операційного дня Центрального депозитарію виключно після виконання процедури звірки балансу.

6.5. Час відкриття та час закриття операційного дня визначений в Правилах Центрального депозитарію цінних паперів.

6.6. Депозитарні установи зобов'язані періодично виходити на зв'язок з інформаційною системою Центрального депозитарію, а саме з ВОД Центрального депозитарію, кожного операційного дня Центрального депозитарію. Періодичність виходу на зв'язок визначена Правилами Центрального депозитарію цінних паперів.

Депозитарна установа, на рахунку якої в Центральному депозитарії обліковуються цінні папери, що заблоковані для торгів на фондовій(их) біржі(ах), та в інших випадках, передбачених Правилами Центрального депозитарію цінних паперів, зобов'язана постійно підтримувати зв'язок з інформаційною системою Центрального депозитарію, а саме з ВОД Центрального депозитарію, протягом кожного операційного дня Центрального депозитарію.

6.7. Протягом сеансу зв'язку ВОД депозитарної установи та ВОД Центрального депозитарію повинно відбутися:

- контроль відповідності програмного та лінгвістичного забезпечення ВОД депозитарної установи еталонам, що зберігаються на ВОД Центрального депозитарію;
- оновлення (у разі необхідності) програмного та лінгвістичного забезпечення ВОД депозитарної установи;
- встановлення зв'язку з операційним днем Центрального депозитарію;
- обмін сеансами, що містять інформацію системи депозитарного обліку (не обов'язково).

6.8. Підтвердженням успішного встановлення зв'язку між депозитарною установою та інформаційною системою Центрального депозитарію, а саме між ВОД депозитарної установи та ВОД Центрального депозитарію, наявність у щоденних протоколах обробки даних на вузлах СОІ Центрального депозитарію та депозитарної установи запису:

Встановлено зв`язок з операційним днем депозитарію.

6.9. У випадку, коли встановлення зв’язку між ВОД депозитарної установи та ВОД Центрального депозитарію неможливе через збій у системі передачі даних, депозитарна установа повинна вжити заходів з відновлення власними силами зв’язку з Центральним депозитарієм з використанням резервних каналів зв’язку у межах того ж операційного дня, коли стався збій.

6.10. У разі, якщо час відновлення телекомунікацій між ВОД депозитарної установи та ВОД Центрального депозитарію виходить за межі одного операційного дня, депозитарна установа повинна письмово повідомити про це Центральний депозитарій та погодити з ним порядок обміну інформацією системи депозитарного обліку на період такого відновлення.

6.11. Операційний день депозитарної установи може бути закритий тільки після проведення процедури звірки балансу з Центральним депозитарієм. У випадку невідповідності балансу, депозитарна установа повинна терміново (в будь-якому разі, не пізніше відкриття наступного операційного дня) повідомити Центральний депозитарій про такий факт, шляхом направлення листа засобами факсимільного зв’язку.

6.12. Ініціювання виконання кожної операції (або комплексу операцій) здійснюється шляхом створення в Модулі Центрального депозитарію та/або в Модулі депозитарної установи відповідного електронного розпорядження та його виконання відповідно до алгоритмів, визначених Центральним депозитарієм.

6.13. Алгоритми виконання операцій в Модулі Центрального депозитарію та Модулі депозитарної установи забезпечують автоматичну синхронізацію інформації системи депозитарного обліку між Центральним депозитарієм та депозитарною установою, тобто відповідність записів на рахунках в цінних паперах на рівні депозитарної установи записам на рахунках в цінних паперах депозитарної установи в Центральному депозитарії.

6.14. Акт функціональної та технічної готовності до роботи в СОІ формується для підписання депозитарною установою одразу ж після здійснення першого успішного сеансу зв’язку з ВОД Центрального депозитарію.

7. Взаємодія Центрального депозитарію та емітента

7.1. У рамках договору про обслуговування випуску цінних паперів Центральний депозитарій та емітент використовують програмні засоби захищеного обміну даними, що входять до складу ППЗ СОІ у таких режимах:

- безпосередній зв’язок «Емітент-Центральний депозитарій» – обмін даними (електронними розпорядженнями та результатами їхньої обробки) в обидва боки;

- зв’язок «Керуючий рахунком у цінних паперах емітента- Центральний депозитарій» – обмін даними (електронними розпорядженнями та результатами їхньої обробки) в обидва боки;
- зв’язок «Емітент-Центральний депозитарій» із залученням депозитарної установи, що є особою, визначеною для надання емітенту реєстру власників іменних цінних паперів – обмін даними між Центральним депозитарієм та депозитарною установою виключно для отримання останньою реєстру власників іменних цінних паперів/переліку власників іменних цінних паперів емітента;

7.2. Для організації безпосереднього зв’язку «Емітент-Центральний депозитарій» емітент повинен:

7.2.1. Надати заяву щодо використання засобів захищеного обміну даними для взаємодії з Центральним депозитарієм,

7.2.2. Надати заяву про приєднання до Умов договору про надання послуг електронного цифрового підпису Акредитованим центром сертифікації ключів Публічного акціонерного товариства «Національний депозитарій України».

7.2.3. Отримати засоби електронного цифрового підпису від Акредитованого центру сертифікації ключів Публічного акціонерного товариства «Національний депозитарій України». Сертифікат відкритого ключа електронного цифрового підпису та сам ключ повинні належати виключно особі, яка має право підпису відповідних документів в паперовому вигляді (розпорядник рахунку).

7.2.4. Отримати від Центрального депозитарію програмні засоби захищеного обміну даними та настроїти їх згідно з інструкцією, що додається до дистрибутива та додатково розміщена на офіційному сайті Центрального депозитарію.

7.2.5. Після встановлення та налагодження програмних засобів захищеного обміну даними емітент повинен встановити з’єднання з ВОД Центрального депозитарію та обмінятися тестовими даними.

7.2.6. Підписати Акт функціональної та технічної готовності до роботи в СОІ, який формується для підписання емітентом одразу ж після здійснення першого успішного сеансу зв’язку з ВОД Центрального депозитарію.

7.3. Для організації зв’язку «Керуючий рахунком у цінних паперах емітента- Центральний депозитарій» Керуючий рахунком повинен:

7.3.1. Надати заяву щодо використання засобів захищеного обміну даними для взаємодії з Центральним депозитарієм,

7.3.2. Надати заяву про приєднання до Умов договору про надання послуг електронного цифрового підпису Акредитованим центром сертифікації ключів Публічного акціонерного товариства «Національний депозитарій України».

7.3.3. Отримати засоби електронного цифрового підпису від Центру сертифікації ключів Публічного акціонерного товариства «Національний депозитарій України». Сертифікат відкритого ключа електронного цифрового підпису та сам ключ повинні належати виключно особі, яка має право підпису відповідних документів в паперовому вигляді (розпорядник рахунку).

7.3.4. Отримати від Центрального депозитарію програмні засоби захищеного обміну даними та настроїти їх згідно з інструкцією, що додається до дистрибутива та додатково розміщена на офіційному сайті Центрального депозитарію.

7.3.5. Після встановлення та налагодження програмних засобів захищеного обміну даними Керуючий рахунком повинен встановити з'єднання з ВОД Центрального депозитарію та обміняться тестовими даними.

7.3.6. Підписати Акт функціональної та технічної готовності до роботи в СОІ, який формується для підписання Керуючим рахунком одразу ж після здійснення першого успішного сеансу зв'язку з ВОД Центрального депозитарію.

7.4. У випадку зв'язку «Емітент-Центральний депозитарій» із залученням депозитарної установи, що є особою, визначеною для надання емітенту реєстру власників іменних цінних паперів, така депозитарна установа на момент укладання з емітентом договору про надання реєстру власників іменних цінних паперів повинна бути учасником СОІ. Для організації зв'язку «Емітент-Центральний депозитарій» із залученням депозитарної установи емітент повинен:

7.4.1. Надати до Центрального депозитарію інформацію щодо депозитарної установи, з якою емітент уклав договір про надання реєстру власників іменних цінних паперів згідно вимог Регламенту провадження депозитарної діяльності Центрального депозитарію цінних паперів та Правил Центрального депозитарію цінних паперів.

7.4.2. Забезпечити виконання обраною депозитарною установою таких заходів:

- отримання від Центрального депозитарію програмних засобів захищеного обміну даними та їх настроювання згідно з інструкцією, що додається до дистрибутива та додатково розміщена на офіційному сайті Центрального депозитарію;
- встановлення з'єднання з ВОД Центрального депозитарію та обмін тестовими даними.

7.4.3. Підписати Акт функціональної та технічної готовності до роботи в СОІ, який формується для підписання депозитарною установою одразу ж після здійснення першого успішного сеансу зв'язку депозитарної установи з ВОД Центрального депозитарію.

7.4.4. Для роботи із засобами захищеного обміну даними використовуються наявні у депозитарної установи засоби електронного цифрового підпису та шифрування.

7.5. Організація захисту інформації під час передавання електронних документів від Центрального депозитарію до емітента покладається на емітента без урахування застосованого режиму зв'язку.

8. Забезпечення безперервності функціонування СОІ

8.1. Безперервність функціонування СОІ забезпечується за рахунок резервування програмного забезпечення та технічних засобів, а також резервного збереження (копіювання) інформації, що обробляється в СОІ.

8.2. Відповідальність за запровадження на ВОД СОІ механізмів резервування програмних та технічних засобів, а також резервного копіювання даних покладається на Учасника СОІ.

8.3. Метою зазначених заходів є забезпечення виконання функцій учасника СОІ в умовах, коли на його діяльність спричиняють вплив несприятливі дестабілізуючі фактори або надзвичайні ситуації.

8.4. Учасник СОІ зобов'язаний мати резервні програмні засоби, засоби обчислювальної техніки, джерела електроживлення, мережеве обладнання, телекомунікаційні канали зв'язку, а також інші технічні засоби, що забезпечують функціонування ВОД СОІ.

8.5. Учасник СОІ зобов'язаний підтримувати в актуальному стані резервне програмне забезпечення, його налаштування, а також засоби захисту інформації.

8.6. Резервне збереження (копіювання) інформації Центральний депозитарій та депозитарна установа виконують кожного операційного дня. Резервне збереження (копіювання) інформації емітентом обирається самостійно в залежності від обсягів інформаційного обміну з Центральним депозитарієм, але не рідше, ніж один раз на місяць.

8.7. Конкретний спосіб, у який буде виконуватись резервування, обирається учасником СОІ таким чином, щоб забезпечити відновлення працездатності ВОД після збою протягом одного операційного дня. У разі наявності об'єктивних обставин, що перешкоджають процесу відновлення і можуть бути підтверджені документально, за погодженням з Центральним депозитарієм термін відновлення може бути подовженим.

8.8. Запровадження механізмів резервного копіювання даних, що циркулюють на ВОД Учасника СОІ є обов'язковим.

8.9. Резервному збереженню (копіюванню), зокрема, підлягають:

- інформаційні масиви (бази даних) системи депозитарного обліку;
- прикладне програмне забезпечення СОІ;
- ключові дані (особисті та відкриті ключі, сертифікати відкритих ключів) посадових осіб учасника СОІ.

8.10. Зберігання резервних копій повинне здійснюватися на зовнішніх машинних носіях даних, у місцях, захищених від впливу магнітного поля чи випромінювання.

8.11. Зберігання резервних копій повинне здійснюватися окремо від зберігання оригінальних інформаційних масивів і на такій відстані, щоб забезпечити встановлений цим Положенням термін відновлення працездатності ВОД.

8.12. Учасник СОІ повинен зберігати не менше, ніж п'ятнадцять останніх резервних копій. Крім цього, повинні зберігатись резервні копії за кожний останній операційний день місяця.

8.13. Резервне збереження (копіювання) повинне супроводжуватись протоколюванням таким чином, щоб результат створення резервної копії був однозначно визначеним. Аналіз протоколів резервного збереження (копіювання) за попередній операційний день має відбуватись після завершення процесу до відкриття наступного операційного дня Центрального депозитарію. У випадку, якщо резервна копія була створена з помилками, учасник СОІ повинен ужити невідкладних заходів із визначення та усунення причин збою, а також створення іншої резервної копії.

8.14. Резервні копії, що зберігаються, не рідше, ніж раз на місяць, повинні проходити тестування шляхом відновлення з однієї резервної копії (на вибір) на тестовій ділянці ВОД Учасника СОІ. У разі негативного результату та з метою визначення та усунення причин збою відновлення, такій же перевірці підлягають всі резервні копії, що зберігаються, у послідовності, починаючи з останньої.

8.15. У випадку виявлення факту несанкціонованого доступу або

пошкодження інформації, що міститься в системі депозитарного обліку, наслідком чого стала втрата або викривлення такої інформації, а також некоректна робота ППЗ СОІ (далі – кризова ситуація), Учасник СОІ повинен протягом того ж операційного дня або не пізніше початку наступного операційного дня здійснити такі дії:

- повідомити Центральний депозитарій про факт настання кризової ситуації;
- вжити заходів щодо виправлення кризової ситуації, а також виявлення та усунення причин, що призвели до такої ситуації;
- повідомити Центральний депозитарій про виправлення кризової ситуації.

8.16. Після виправлення кризової ситуації необхідно провести розслідування причин виникнення кризової ситуації. Для цього необхідно провести внутрішнє розслідування для з'ясувати наступних обставин:

- випадкова або навмисна кризова ситуація?
- чи враховувалася можливість її виникнення в плані захисту інформації ІТС?
- чи можливо було її передбачити?
- чи викликана вона слабкістю засобів захисту і реєстрації?
- чи перевищив збиток від неї встановлений рівень?
- чи є непоправний збиток і який його орієнтовний розмір?
- чи це перша кризова ситуація такого роду?
- чи є можливість точно визначити коло винних у спричиненні даної ситуації?
- в чому причина кризової ситуації?
- чи достатньо наявного резерву?
- чи є необхідність перегляду плану захисту?
- чи є необхідність перегляду Плану захисту інформації ІТС?

Відповідальними за розслідування є керівник підрозділу із захисту інформації або, за відсутності останнього, – керівник підрозділу інформаційних технологій. Звіт про результати розслідування і пропозиції щодо вдосконалення ІТС надаються керівнику Учасника СОІ.

8.17. У разі, якщо кризова ситуація пов'язана з пошкодженням актуальності або логічної несуперечності інформаційних масивів (бази даних) ВОД Центрального депозитарію та ВОД Учасника СОІ, а також у разі втрати інформації чи технічних засобів ВОД Учасника СОІ, Центральний депозитарій тимчасово блокує доступ цього Учасника СОІ до своєї інформаційної системи.

8.18. Доступ Учасника СОІ до інформаційної системи Центрального депозитарію відновлюється після повідомлення Учасника СОІ про виправлення кризової ситуації та позитивного результату перевірки Центральним депозитарієм актуальності та несуперечності інформаційних масивів (бази даних) ВОД Центрального депозитарію та ВОД Учасника СОІ (звірки настроювань, довідників, балансу тощо).

9. Захист інформації

9.1. Інформація, що циркулює в СОІ, поділяється на відкриту та інформацією з обмеженим доступом. Інформація з обмеженим доступом, що циркулює в СОІ, має статус «конфіденційної інформації».

9.2. Відкрита інформація під час обробки в СОІ повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

9.3. Під час обробки в СОІ конфіденційної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

9.4. Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам СОІ. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

9.5. У СОІ забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

9.6. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до конфіденційної інформації та її обробки, контроль за цілісністю засобів захисту в СОІ повинне здійснюватися автоматизованим способом.

9.7. Передача конфіденційної інформації між ВОД відкритими каналами зв’язку здійснюється лише у зашифрованому вигляді із застосуванням засобів КЗІ, що мають сертифікат відповідності (експертний висновок), за результатами державної експертизи в галузі КЗІ (атестат відповідності).

9.8. Згідно із законом захисту в СОІ підлягають:

- дані системи депозитарного обліку у вигляді окремих файлів або об’єктів баз даних;
- персональні дані фізичних осіб у вигляді окремих файлів або об’єктів баз даних;

9.9. Крім визначеного в п.9.8 переліку, захисту в СОІ підлягають інші програмні та інформаційні ресурси ВОД Учасника, зокрема:

- програмне забезпечення ВОД;
- файли конфігурації програмного та апаратного забезпечення;
- журнали реєстрації подій;
- особисті ключі фізичних осіб.

9.10. Учасник СОІ повинен забезпечити захист інформації, перелік якої наведений у пп.9.8, 9.9 цього Положення, шляхом створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи Учасника СОІ та підтвердження її відповідності вимогам нормативних документів системи технічного захисту інформації (атестації) у встановленому законодавством порядку.

9.11. В комплексній системі захисту інформації інформаційно-телекомунікаційної системи Учасника СОІ мають бути визначені, зокрема, такі об’єкти захисту, що перелічені у пп. 9.8, 9.9 цього Положення.

9.12. У складі комплексної системи захисту інформації інформаційно-телекомунікаційної системи Учасника СОІ повинні застосовуватись організаційні та інженерно-технічні заходи, засоби та методи захисту інформації. Серед інших, учасник СОІ в складі ВОД повинен застосовувати засоби антивірусного захисту.

9.13. Учасник СОІ повинен підтвердити свою спроможність відповідати вимогам цього Положення щодо технічного та програмного забезпечення, а також забезпечення захисту конфіденційної інформації. Відповідність ІТС Учасника СОІ визначеним цим Положенням вимогам перевіряється за рішенням керівництва Центрального депозитарію але не частіше, ніж раз на два роки, а також позапланово – у разі отримання відомостей про можливу невідповідність зазначеним вимогам.

9.14. Контролю з боку Центрального депозитарію підлягають, зокрема, такі компоненти ІТС Учасника СОІ:

- склад апаратного та програмного забезпечення ІТС;
- об’єкти захисту, суб’єкти доступу до захищених ресурсів та атрибути такого доступу;
- налаштування комплексу засобів захисту від несанкціонованого доступу;

- антивірусне програмне забезпечення;
- дотримання вимог до фізичного середовища.

Зазначений контроль здійснюється з урахуванням експертного висновку на комплексну систему захисту інформації Учасника СОІ.

У разі підключення Учасника СОІ до комплексної системи захисту інформації Центрального депозитарію, контроль повинен здійснюватися за відповідною інструкцією, що входить до складу документації на комплексну систему захисту інформації ІТС Центрального депозитарію.

9.15. Відповідальність за забезпечення захисту інформації з обмеженим доступом, що циркулює у ВОД Центрального депозитарію, покладається на Центральний депозитарій. Відповідальність за забезпечення захисту інформації з обмеженим доступом, що циркулює на ВОД Учасника СОІ, покладається на відповідного Учасника СОІ.

9.16. Надання послуг ЕЦП, а також забезпечення Учасників СОІ надійними засобами ЕЦП, здійснюється Центральним депозитарієм на договірних засадах.

9.17. Порядок надання послуг ЕЦП Учасникам СОІ під час провадження ними діяльності визначається Регламентом роботи АЦСК Публічного акціонерного товариства «Національний депозитарій України» та умовами договору між учасником СОІ та Центральним депозитарієм про надання таких послуг.

10. Перелік та опис програмного забезпечення, яке використовується Центральним депозитарієм у правовідносинах, що виникають під час провадження ним професійної діяльності

Для здійснення професійної діяльності Центральний депозитарій використовує нижченаведені програмні засоби:

10.1. Для серверів:

- операційна система Microsoft Windows Server (2003 R2, 2008 R2, 2012);
- програмний продукт депозитарного обліку (Модуль Центрального депозитарію, серверна частина);
- програмні засоби захищеного обміну даними;
- системи керування базами даних Oracle та Microsoft SQL Server;
- засоби електронного цифрового підпису та криптографічного захисту інформації;
- програмні засоби організації доступу до мережі Інтернет, розмежування доступу, електронної пошти;
- програмне забезпечення загальне (антивіруси для серверів, архіватори, засоби перегляду файлів різних форматів).

10.2. Для робочих станцій:

- операційна система Microsoft Windows XP Professional або Microsoft Windows 7 Professional;
- програмний продукт депозитарного обліку (Модуль Центрального депозитарію, клієнтська частина);
- офісний пакет Microsoft Office;
- засоби електронного цифрового підпису та криптографічного захисту інформації;
- програмне забезпечення загальне (антивіруси для робочих станцій, архіватори, засоби перегляду файлів різних форматів тощо).

11. Вимоги до програмного та технічного обладнання Учасника СОІ

11.1. Програмне забезпечення ВОД Учасника СОІ поділяється на:

11.1.1. Системне програмне забезпечення: операційні системи, системи керування базами даних, офісне.

11.1.2. Прикладне програмне забезпечення (ППЗ): модуль депозитарної установи, засоби захищеного обміну даними тощо.

11.1.3. Загальне програмне забезпечення: антивіруси, архіватори, засоби перегляду файлів різних форматів тощо.

11.2. Вимоги до системного програмного забезпечення учасника СОІ:

11.2.1. 32-х розрядні операційні системи Microsoft Windows XP Professional або Microsoft Server 2003 усіх модифікацій.

11.2.2. Використання ППЗ СОІ під керуванням 64-х розрядних операційних систем сімейства Windows чи операційних систем Microsoft Windows 7 або Microsoft Server 2008 можливо лише за умови його розгортання у рамках будь-якого із засобів віртуалізації. Штатні безкоштовні засоби віртуалізації, що рекомендуються:

11.2.3. XP Mode (для Windows 7 Professional та вище);

11.2.4. Hyper-V (для Windows Server 2008).

11.3. 32-х та 64-х розрядні СКБД, що підтримуються:

- Oracle від версії 9i до 10g Release 2 версія 10.2.0.4 включно;
- Microsoft SQL Server від версії 2000 до 2008 включно.

11.4. Офісне програмне забезпечення, що підтримується:

- Microsoft Office 2003, 2007, 2010.

11.5. До прикладного та загального програмного забезпечення окремих вимог не висувається. Перелік загального програмного забезпечення, що

використовується спільно з ППЗ СОІ, має бути погодженим з Центральним депозитарієм.

11.6. Вимоги до технічного обладнання Учасника СОІ:

11.6.1. Робоча станція, на якій функціонує ППЗ СОІ:

- мінімальна конфігурація (процесор: Intel Pentium 4; тактова частота: 1,5 ГГц; оперативна пам'ять 512 Мбайт; пристрій архівування даних на зовнішні носії);
- рекомендована конфігурація (процесор: Intel Core 2 Duo; тактова частота: 2 ГГц; оперативна пам'ять 1 Гбайт; дисковий масив RAID; пристрій архівування даних на зовнішні носії).

11.6.2. Мінімальні та рекомендовані параметри до обладнання серверу баз даних висуваються виробниками СКБД, перелік яких наведено у п.12.3 цього Положення.

11.7. У випадку експлуатації ППЗ СОІ та СКБД на одному комп'ютері вимоги до такого комп'ютера на 30% перевищують вимоги до серверу СКБД.

11.8. Вимоги до телекомунікаційного обладнання Учасника СОІ:

- Інтернет-канал, що забезпечує гарантовану швидкість передачі даних не нижче, ніж 128 Кбіт/с;
- фіксована IP-адреса;
- безпосередній Інтернет-доступ до TCP-портів серверу Центрального депозитарію (номер порту визначається конкретним ППЗ СОІ);
- локальна обчислювальна мережа, що забезпечує інформаційний обмін між робочими станціями та сервером (серверами) зі швидкістю передачі даних не нижче, ніж 100 Мбіт/с.

11.9. У разі зміни IP-адреси Учасник СОІ повинен протягом двох годин після виявлення такої зміни повідомити про це Центральний депозитарій та надати дані щодо нової IP-адреси.

11.10. Акт функціональної та технічної готовності до роботи в СОІ підписується лише після встановлення Центральним депозитарієм відповідності програмного та технічного обладнання Учасника СОІ зазначеним вище вимогам.

11.11. Для забезпечення постійного підвищення рівня надійності та ефективності функціонування СОІ Центральний депозитарій може змінювати програмно-технологічну структуру системи, алгоритми обробки інформації, шляхи програмно-технічної реалізації її елементів, а також вимагати від Учасників СОІ відповідної адаптації їх програмно-технічних засобів. Терміни інформування Учасників СОІ про необхідність такої адаптації визначаються Центральним депозитарієм.