**Щодо захисту інформації, що міститься**

**в системі депозитарного обліку Депозитарної установи**

1. **Щодо комплексної системи захисту інформації (КСЗІ) та отримання Атестату відповідності.**

Згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації (ст.1 «Визначення термінів»)

Порядок створення комплексної системи захисту інформації передбачає наступні заходи.

Виконавцем робіт із створення комплексної системи захисту інформації (далі - КСЗІ) в інформаційно-телекомунікаційній системі (далі - ІТС) може бути суб’єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації (далі - ТЗІ), необхідність проведення якого визначено технічним завданням на створення КСЗІ.

Для проведення інших видів робіт з ТЗІ, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення КСЗІ необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензію на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Створення КСЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" на підставі технічного завдання (далі - ТЗ), розробленого згідно з вимогами нормативного документу системи технічного захисту інформації  НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі".

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів тощо;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації.

Для формування загальних вимог до КСЗІ в ІТС здійснюється обґрунтування необхідності її створення на підставі вимог законодавства, що встановлюють обов’язковість забезпечення конфіденційності, цілісності і доступності інформації, та обстеження середовищ функціонування ІТС - обчислювальної системи, фізичного середовища, середовища користувачів, оброблюваної інформації і технології її обробки.

За результатами детального вивчення об’єкта, на якому створюється КСЗІ, уточнення моделі загроз та моделі порушника, результатів аналізу можливості керування ризиками здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій та документальне оформлення політики безпеки.

Технічне завдання на створення КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС у вигляді окремого розділу ТЗ на створення ІТС, окремого (часткового) ТЗ або доповнення до ТЗ на створення ІТС.

В ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою ІТС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Проект КСЗІ розробляється на підставі та у відповідності до ТЗ. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. У результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Введення КСЗІ в дію включає розробку розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС, створення служби захисту інформації, розробку і затвердження Плану захисту інформації, навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та адміністраторів), комплектування КСЗІ засобами захисту інформації, матеріалами, обладнанням, проведення будівельно-монтажних та пусконалагоджувальних робіт, попередніх випробувань та дослідної експлуатації КСЗІ.

Під час попередніх випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Під час дослідної експлуатації:

- відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

- співробітники служби захисту інформації та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

- здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування комплексу засобів захисту інформації від несанкціонованого доступу;

- здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами дослідної експлуатації приймається рішення про готовність КСЗІ в ІТС до представлення на державну експертизу.

Проведення експертизи Держспецзв’язку для підтвердження відповідності системи захисту інформації депозитарних установ (в т.ч. банків) вимогам нормативних документів системи технічного захисту інформації встановленому законодавством у наступному порядку.

Для проведення експертизи КСЗІ в ІТС або засобу технічного захисту інформації (далі - засіб ТЗІ) Замовник надсилає заяву встановленої форми на ім’я Голови (заступника Голови) Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку) за адресою: 03680, Київ, вул. Солом’янська, 13.

За результатами розгляду заяви у місячний термін приймається рішення про можливість й доцільність проведення експертизи та визначення підрозділу Держспецзв’язку, підприємства, установи або організації, які проводитимуть експертизу (далі - Організатор експертизи),.

Відносини між Замовником і Організатором експертизи регламентуються укладеним між ними договором про проведення експертизи. Термін проведення експертизи визначається договором і не повинен перевищувати шести місяців. У разі значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації Держспецзв’язку та Замовника.

Замовник надає Організатору експертизи комплект організаційно-технічної документації на КСЗІ в ІТС або засіб ТЗІ, необхідний для проведення експертних випробувань.

 Організатор експертизи, за результатами аналізу наданих Замовником документів і з урахуванням загальних методик оцінювання задекларованих характеристик об’єкта експертизи, формує програму і окремі методики проведення експертизи та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.

Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в інформаційно-телекомунікаційних системах Адміністрації Держспецзв’язку, а окремі методики - з зазначеним департаментом.

Терміни розробки окремих методик та необхідного програмно-технічного забезпечення залежать від характеру та складності об’єкта експертизи і визначаються у договорі на проведення експертизи.

Результати експертних робіт за окремими методиками оформлюються у вигляді протоколу виконання робіт, затвердженого Організатором експертизи.

У разі виявлення невідповідності об’єкта експертизи вимогам нормативних документів з ТЗІ, Організатор експертизи може запропонувати Замовнику виконати доробку КСЗІ в ІТС або засобу ТЗІ. Терміни доробки визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором експертизи.

Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

За результатами проведених робіт Організатор експертизи складає експертний висновок щодо відповідності КСЗІ в ІТС або засобу ТЗІ вимогам нормативних документів з ТЗІ і разом з протоколом виконання робіт з подає до Адміністрації Держспецзв’язку.

1. **Система захисту інформації, створена депозитарною установою.**

Комплекс системи захисту інформації, впроваджений Депозитарною установою, відповідає вимогам чинного законодавства, зокрема, Порядку обігу, зберігання та знищення електронних документів, що використовуються професійними учасниками депозитарної системи України, затвердженому Рішення НКЦПФР 27.12.2013 № 2996, а також вимогам, встановленим Центральним депозитарієм та Національним банком.

До комплексу заходів, які організовані Депозитарною установою, по захисту інформації входять заходи та засоби, які реалізують способи, методи та механізми захисту інформації.

1. Депозитарна установа має:

* два незалежних джерела електроживлення, а також джерела додаткового безперервного електроживлення на випадок зникнення електричного струму в електромережі;
* програмно-технічний комплекс, який забезпечить виконання вимог, установлених Комісією для цієї діяльності, у тому числі забезпечить виконання вимог щодо взаємодії депозитарної установи з Центральним депозитарієм та подання до Комісії адміністративних даних та інформації у вигляді електронних документів із застосуванням електронного цифрового підпису.

Депозитарна установа обладнана системними і програмно-технічними засобами та засобами зв'язку, які запобігають втратам, крадіжкам, несанкціонованому знищенню, викривленню, підробленню, копіюванню інформації і відповідати вимогам міжнародних та національних стандартів.

Депозитарна установа забезпечує резервне збереження (копіювання) інформації у порядку та відповідно до складу, визначених нормативно-правовим актом Комісії, який регулює порядок провадження депозитарної діяльності.

Носії з архівними даними стану рахунків зберігаються у сховищі.

2. Депозитарна установа розробила та затвердила документи, передбачені нормативно-правовим актом Комісії що регулює порядок провадження депозитарної діяльності.

1. **Вимоги, що висуваються до депозитарної установи Центральним депозитарієм.**

Згідно статті 27 Закону України «Про депозитарну систему України», захист інформації, що міститься у системі депозитарного обліку, забезпечується внаслідок використання електронного документообігу; при цьому порядок обігу, зберігання та знищення електронних документів, що використовуються професійними учасниками депозитарної системи України, встановлюється Комісією. Такий порядок, затверджений Рішенням НКЦПФР від 27.12.2013 р. № 2996, передбачає наступне:

* Інформаційна діяльність професійних учасників депозитарної системи України здійснюється в рамках правовідносин між Центральним депозитарієм та депозитарними установами, права та обов'язки яких визначаються *на договірних засадах* з урахуванням вимог, встановлених нормативно-правовими актами НКЦПФР.
* Для здійснення інформаційної діяльності професійні учасники депозитарної системи України використовують інформаційно-телекомунікаційну систему обробки інформації Центрального депозитарію (ІТС ЦД).
* Функції з обігу (створення, оброблення, відправлення, передавання, одержання) електронних документів, їх зберігання та знищення виконуються професійними учасниками депозитарної системи України та реалізуються *в програмному забезпеченні ІТС ЦД.*
* У ІТС ЦД повинен забезпечуватись захист інформації, яка в цій системі обробляється та зберігається, шляхом створення *комплексної системи захисту інформації з підтвердженою відповідністю* у встановленому законодавством України порядку.
* Функції оброблення електронних документів реалізовані в прикладному програмному забезпеченні ІТС ЦД.
* Професійні учасники депозитарної системи України отримують послуги ЕЦП від акредитованого центру сертифікації ключів.

Депозитарні установи мають виконувати вимоги цього Порядку, Положення про інформаційно-телекомунікаційну систему обробки інформації Центрального депозитарію цінних паперів (Положення про СОІ, <http://csd.ua/images/stories/pdf/polozhennya_pro_coi_20130920.pdf>), типового депозитарного договору між депозитарною установою і Центральним депозитарієм (вимоги до якого врегульовані рішенням НКЦПФР від 06.08.2013 № 1410), Ліцензійних умов провадження депозитарної діяльності (рішення НКЦПФР від 21.05.2013 № 862), інших нормативно-правових документів та документів Центрального депозитарію.

Зокрема, відповідно до п. 9.13 Положення про СОІ, депозитарна установа (учасник СОІ) повинна підтвердити свою спроможність відповідати вимогам цього Положення щодо технічного та програмного забезпечення, а також забезпечення захисту конфіденційної інформації. А Центральний депозитарій, відповідно до п. 9.14 контролює ЕТС учасника СОІ, а саме:

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.

Фактично, **з огляду на безальтернативність для депозитарної установи отримання послуг від Центрального депозитарію для провадження ліцензованої професійної діяльності, депозитарна установа в обов’язковому порядку користується засобами ІТС ЦД, в т.ч. програмним забезпеченням «ОБЕРОН», застосовує для забезпечення захисту інформації в системі депозитарного обліку ІТ-складову КСЗІ, створеної Центральним депозитарієм, отримує послуги електронного цифрового підпису від Центрального депозитарію (як акредитованого центру сертифікації ключів) тощо.**

При цьому на веб-сайті Центрального депозитарію оприлюднено (<http://www.csd.ua/index.php?option=com_content&view=article&id=84&Itemid=59&lang=ua>) **Атестат відповідності від 25.05.2015 р. № 12472**, який свідчить, що комплексна система захисту інформації ІТС ЦД забезпечує захист інформації відповідно до вимог нормативних документів системи технічного захисту інформації України. Цей Атестат відповідності зареєстрований Державною службою спеціального зв’язку та захисту інформації України (Держспецзв’язку) та дійсний до 25.05.2020 р.

1. **Особливості КСЗІ Центрального депозитарію.**

Як вже зазначалося, для депозитарної установи є обов’язковим застосовувати у власній ІТС, а відповідно включати до складу власної КСЗІ елементи КСЗІ Центрального депозитарію, зокрема, клієнтську частину програмного продукту депозитарного обліку «ОБЕРОН».

Разом з тим, Центральний депозитарій надає для ознайомлення тільки Атестат відповідності, оприлюднюючи його на офіційному веб-сайті. Натомість експертний висновок та інші технічні документи, пов’язані із створенням КСЗІ Центрального депозитарію, в публічному доступі відсутні, напевне, через те, що мають обмежений доступ.

Через відсутність такої інформації взагалі є сумніви щодо того, чи входить документація щодо клієнтської частини програмного продукту «ОБЕРОН», якою безумовно користуються депозитарні установи, до складу експертної документації КСЗІ Центрального депозитарію, чи поширюється Атестат відповідності на цей програмний продукт.

**За відсутності доступу до експертної документації КСЗІ Центрального депозитарію неможливо отримати експертний висновок та атестат відповідності КСЗІ в ІТС депозитарної установи.**

1. **Вимоги, що висуваються до депозитарної установи Національним банком.**

При взаємодії депозитарних установ з Національним банком України в ході депозитарного обліку державних та муніципальних цінних паперів депозитарні установи мають відповідати вимогам нормативно-правових документів Національного банку щодо захисту інформації, які суттєво відрізняються від вимог, зазначених в документах Центрального депозитарію та Держспецзв’язку.

Відповідно до депозитарного договору (<https://bank.gov.ua/doccatalog/document?id=36873272>), депозитарні установи використовують засоби захисту інформації Національного банку та мають дотримуватися порядку отримання, обліку, передавання, використання та зберігання засобів криптозахисту Національного банку та виконання правил інформаційної безпеки відповідно до нормативно-правових актів Національного банку з питань організації захисту електронних банківських документів в установах, яким надано право доступу до інформаційно-обчислювальної мережі Національного банку, та інших вимог, визначених законодавством України, а також виконувати вимоги захисту електронних депозитарних документів щодо технічних, програмних та організаційних засобів захисту інформації.

Відповідність зазначеним вимогам періодично перевіряється Національним банком.

Відмінності у вимогах стосуються підходів до каналів зв’язку, форматів та засобів захисту інформації в ІТС та документообігу.

У разі, якщо депозитарна установа обслуговується Національним банком в ході проведення депозитарних операцій з державними та муніципальними цінними паперами, для депозитарної установи є обов’язковим застосовувати у власній ІТС, а відповідно включати до складу власної КСЗІ елементи КСЗІ Національного банку, зокрема, щодо захисту інформації.

**Зрозуміло, що відмінності програмних продуктів та вимог до захисту інформації при взаємодії з Центральним депозитарієм та Національним банком додатково ускладнюють завдання створення КСЗІ в депозитарній установі та отримання Атестату відповідності.**

**Аналогічні проблеми виникають не тільки в небанківських установ, але й в банків, які також мають вирішувати завдання застосування в КСЗІ суперечливих вимог та документів Національного банку, Центрального депозитарію та Держспецзв’язку.**

1. **Висновок.**

Депозитарною установою створено комплекс заходів по захисту інформації при провадженні депозитарної діяльності.

Однак, через об’єктивні причини (суперечливість правової бази щодо захисту інформації, обмеженість функціоналу КСЗІ Центрального депозитарію в частині клієнтської частини програмного продукту для депозитарних установ та недоступність експертної документації для депозитарних установ), Держспецзв’язок наразі не має можливості підтвердити відповідність систем захисту інформації депозитарних установ (особливо банків) вимогам нормативних документів системи технічного захисту інформації у встановленому законодавством порядку.