Голові Національного банку України
ГОНТАРЕВІЙ В.О.

Щодо комплексної системи захисту
інформації в депозитарній системі

Шановна Валеріє Олексіївно!

Асоціація «Українські фондові торговці» є саморегулівною організацією професійних учасників фондового ринку і об’єднує депозитарні установи.

Рішенням Національної комісії з цінних паперів та фондового ринку (далі – НКЦПФР) «Щодо захисту інформації, що міститься в системі депозитарного обліку, при її обробці в інформаційно-телекомунікаційних системах депозитарних установ» № 149 від 07.03.2017 (далі – Рішення № 149) депозитарні установи, в т.ч. банки, зобов’язано провести обстеження середовища функціонування інформаційно-телекомунікаційних систем (далі – ІТС), які використовуються в професійній діяльності, та впровадити комплексні системи захисту інформації (далі – КСЗІ) з підтвердженою відповідністю у встановленому законодавством України порядку.

Рішення № 149 посилається на вимоги ч. 1 ст. 24 Закону України «Про депозитарну систему України», ст. ст. 8 та 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», п. 2 розд. IX Положення про провадження депозитарної діяльності, затвердженого рішенням НКЦПФР від 23.04.2013 № 735 та зареєстрованого в Мінюсті України 27.06.2013 за № 1084/23616.

Разом з тим, практична реалізація Рішення № 149 викликає низку питань.

По-перше, відповідно до Порядку створення КСЗІ, проведення експертизи та видачі Експертних висновків і Атестатів відповідності, Порядку проведення робіт із створення КСЗІ в ІТС (НД ТЗІ 3.7-003-2005), затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08.11.2005 № 125 (далі – ДСТЗІ), Методичними вказівками щодо розробки технічного завдання на створення КСЗІ в автоматизованій системі, затверджених наказом ДСТЗІ від 28.04.1999 № 22, ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97 та ДБH А.2.2-2-96, створення КСЗІ складається з таких етапів:

1. формування загальних вимог до КСЗІ в ІТС, що передбачає в т.ч., обстеження середовищ функціонування ІТС, зокрема загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо), види і характеристики каналів зв'язку. Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості;
2. розробка політики безпеки інформації в ІТС;
3. розробка технічного завдання на створення КСЗІ;
4. розробка проекту КСЗІ;
5. введення КСЗІ в дію та оцінка захищеності інформації в ІТС;
6. супроводження КСЗІ.

Такі дії здійснюються за допомогою осіб, що мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації та технічного захисту інформації.

Відповідно ст. 28 Закону України «Про депозитарну систему України» державне регулювання у депозитарній системі України здійснює Комісія з цінних паперів та фондового ринку, а також Національний банк України та інші державні органи у межах своїх повноважень, визначених законом.

Відповідно до ст. 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» Національний банк України встановлює особливості захисту інформації в системах, які забезпечують банківську діяльність.

Відповідно до п. 4 та 7 ст. 7 Закону України «Про Національний банк України» саме Національний банк України встановлює для банків правила захисту інформації, коштів та майна, визначає напрями розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним облікових систем, контролює створення систем автоматизації банківської діяльності та засобів захисту банківської інформації.

На сьогоднішній день, НБУ встановив регулювання відносин захисту інформації відмінне від регулювання Державної служби спеціального зв’язку та захисту інформації (далі – Держспецзв’язок). При цьому, оскільки депозитарна діяльність банківськими установами здійснюється як частина організаційно-адміністративних та технічних процесів банківської діяльності, з метою виконання вимог Держспецзв’язку при створенні КСЗІ депозитарної установи необхідним буде розкриття відомостей про механізми захисту інформації створені в рамках вимог профільного регулятора. Разом з тим, відповідно до вимог НБУ, неприпустимим є не лише втручання, а й розкриття особливостей роботи таких системи захисту інформації в банківських установах.

Просимо повідомити, чи буде застосовуватись з боку НБУ відповідні санкції до банківських установ, що здійснюють депозитарну діяльність, внаслідок виконання ними Рішення № 149?

По-друге, НБУ, окрім ролі регулятора, також безпосередньо здійснює депозитарну діяльність депозитарія цінних паперів. Технічним інструментом взаємодії НБУ з професійними учасниками фондового ринку є розроблений ним програмний комплекс – Система «ОВДП-online» з окремими каналами зв’язку.

В роботі з банками також використовується й програмно-технологічне забезпечення СертЛайн. Інформація про такі програмні комплекси та канали зв’язку також буде необхідною для створення КСЗІ.

На підготовчому етапі впровадження КСЗІ має здійснюватись аналіз умов функціонування підприємства, засобів забезпечення інформаційної діяльності, які мають вихід за межі підприємства, інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації.

В своєму Рішенні № 149 НКЦПФР рекомендує НБУ забезпечити надання депозитарним установам необхідної інформаційної підтримки та технічної документації щодо наданих їм у користування НБУ для виконання ними професійної діяльності програмних продуктів та інших засобів передавання та (або) оброблення інформації.

Враховуючи таке, на виконання рекомендацій НКЦПФР та з метою визначення вимог для побудови КСЗІ депозитарних установ та інформування членів Асоціації – депозитарних установ просимо надати таку інформацію:

1. копії документів, які визначають порядок підключення та регламент обміну інформацією між депозитарними установами та депозитарієм Національного банку України;
2. копії атестатів відповідності на КСЗІ інформаційно-телекомунікаційної системи депозитарію Національного банку України, з якою взаємодіють депозитарні установи;
3. копії експертних висновків у сфері технічного та/або криптографічного захисту інформації на програмне забезпечення, яке використовується для обміну між інформаційно-телекомунікаційною системою депозитарієм Національного банку України та депозитарними установами;
4. копію технічного завдання на створення Системи «ОВДП-online»;
5. технічну інформацію про канали зв’язку використовувані Системою «ОВДП-online».

Крім того, просимо повідомити, чи погоджувалось Рішення № 149 НКЦПФР з позицією НБУ та чи враховано особливості регулювання захисту інформації в банківській діяльності при прийнятті такого Рішення № 149?

В свою чергу вважаємо за необхідне відзначити значний вклад Національного банку України в формуванні ефективних систем захисту інформації на фінансових ринках.

З повагою

Президент Н.А. ГУРЖИЙ

вик. Дюговський О.С. 044.500.18.92