

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СФЕРИ ПУБЛІЧНОЇ ФІНАНСОВОЇ ДІЯЛЬНОСТІ

Функціонування досконалого механізму забезпечення інформаційної безпеки є однією з ознак правової держави та громадянського суспільства. Такий механізм сприяє реалізації покладених на органи державної влади та місцевого самоврядування повноважень, в тому числі й у сфері публічної фінансової діяльності.

Незважаючи на важливість зазначеного, проблематика забезпечення інформаційної безпеки сфери публічної фінансової діяльності, окремо науковцями не розглядалася.

Розгляд зазначеного питання також актуалізується у зв'язку з прийняттям останнім часом відповідних норм у Податковому кодексі України від 02.12.2010 р. № 2755-VI (ПК України), Законах України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI, «Про відкритість використання публічних коштів» від 11.02. 2015 р. 183-VIII. У результаті ретельного вивчення змісту норм зазначеного законодавства та Закону України «Про інформацію» від 02.10. 1992 р. № 2657-XII, вважаємо, що сутністю діяльності із забезпечення інформаційної безпеки у аналізованій сфері є захист інформації, тобто сукупності відомостей і даних, що створені або отримані у процесі публічної фінансової діяльності її учасниками і необхідні для реалізації покладених на них завдань і функцій.

Результатом ефективної діяльності із забезпечення інформаційної безпеки сфери публічної фінансової діяльності, на нашу думку, має бути функціонування такого механізму, який спрямований на вільне одержання, використання, поширення, зберігання і захист інформації у цій сфері [1]. А тому основними напрямками зазначеної діяльності вважаємо забезпечення доступності інформації у сфері публічної фінансової діяльності та її захист.

Реалізація права на інформацію передбачає певний зв'язок між реальною її доступністю та режимом доступу до неї і, відповідно, доступність інформації обумовлена не лише її юридичним статусом, а й фактичними умовами її використання для різних суб'єктів [2] та специфікою сфери публічної фінансової діяльності. Так, відповідно до ст. 21 ПК України посадові особи контролюючих органів зобов'язані не допускати розголошення

інформації з обмеженим доступом, що одержується, використовується, зберігається під час реалізації функцій, покладених на такі органи, а також надавати органам державної влади та органам місцевого самоврядування на їх письмовий запит відкрити податкову інформацію в порядку, встановленому законом. Разом з тим, у ст. 5 Закону України «Про доступ до публічної інформації» визначено особливості використання публічної інформації з обмеженим доступом і виключний перелік інформації, до якої не може бути обмежено доступ і яка стосується: розпорядження бюджетними коштами; володіння, користування чи розпорядження державним, комунальним майном; умов отримання цих коштів чи майна тощо. Однак аналізована стаття містить застереження, що зазначені положення не поширюються на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Безперечно, надзвичайно важливим стало прийняття Закону України «Про відкритість використання публічних коштів», який визначив умови та порядок забезпечення доступу до інформації про використання публічних коштів розпорядниками та одержувачами коштів державного і місцевих бюджетів, суб'єктами господарювання державної і комунальної власності, фондами загальнообов'язкового державного соціального страхування. Відповідно до цього Закону зазначена інформація готується розпорядниками та одержувачами коштів Державного бюджету України, бюджету Автономної Республіки Крим і місцевих бюджетів, органами Пенсійного фонду, підприємствами, а також фондами загальнообов'язкового державного соціального страхування та подається ними для оприлюднення на єдиному веб-порталі використання публічних коштів.

Також особливого захисту потребує інформація даних про платників податків, відповідно контролюючі органи мають забезпечити достовірність таких даних в Єдиному банку даних про платників податків - юридичних осіб та Державному реєстрі фізичних осіб - платників податків, реєстрі платників податку на додану вартість, реєстрі неприбуткових організацій та інших реєстрах, що формуються та ведуться контролюючими органами згідно з ПК України, їх захист від несанкціонованого доступу, оновлення, архівування та відновлення даних.

З урахуванням зазначеного, основними проблемами забезпечення інформаційної безпеки сфери публічної фінансової діяльності вважаємо неузгодженість правових норм різних законів України щодо доступу до інформації у цій сфері, її захисту, а також відсутність норм, які б містили чіткі механізми реалізації таких норм, забезпечення права на доступ до інформації у сфері публічної фінансової діяльності, контроль за реалізацією цього права, притягнення до відповідальності посадових осіб за недотри-

мання чинного законодавства, що регулює відносини у сфері забезпечення доступу до такої інформації та її захисту.

Подальші дослідження доцільно спрямувати на теоретико-методологічне обґрунтування особливостей забезпечення інформаційної безпеки у окремих сферах публічної фінансової діяльності – бюджетній, податковій, банківській.

Література

1. Дмитренко Е.С. Місце інформаційного забезпечення у системі фінансової безпеки держави / Е. С. Дмитренко // Інформаційна безпека людини, суспільства, держави. – 2011. – №3 (7). – С. 13-17.

2. Дмитренко Е.С. Реалізація права на податкову інформацію у контексті Податкового кодексу України / Е. С. Дмитренко // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 99-104.

УДК 340.134::351

Дмитренко Ю. П.

кандидат юридичних наук, професор
Національна академія СБ України

СОЦІАЛЬНО-ПРАВОВІ ПРОБЛЕМИ КОМПЛЕКТУВАННЯ ПІДРОЗДІЛІВ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ І КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя у багатьох державах приділяється значна увага створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх та внутрішніх загроз кібернетичного характеру.

У провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційно-функціональні структури, що здатні в короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [1, с. 312]. В Україні також відбувається становлення системи забезпечення кібернетичної безпеки. Проте, вірус Petya, яким було вражено значну кількість інформаційних ресурсів органів державної влади України, показав недосконалість національної системи кібербезпеки, виявив суттєві недоліки в організації діяльності кадрового забезпечення її суб'єктів. Приклади кібератак зі спробами втручання в електронну виборчу систему, зокрема під час проведення виборів у різних країнах (навіть США та ін.) визначають надзвичайну актуальність цієї теми. В умовах ведення «гібридної війни» Російською Федерацією проти Украї-