УДК 342.9

ЕЛЕКТРОННІ РЕЄСТРИ ТА ІНФОРМАЦІЙНІ СИСТЕМИ: ПРІОРИТЕТИ, ВИКЛИКИ ТА ЗНАЧЕННЯ ДЛЯ ПУБЛІЧНОГО УПРАВЛІННЯ

Віталій ТОЛУБ'ЯК
заступник начальника Головного управління Пенсійного фонду України в Тернопільській області, доктор наук з державного управління, професор

Олександр ТОМЧУК
начальник управління інформаційних систем та електронних реєстрів Головного управління Пенсійного фонду України в Тернопільській області, магістр з державного управління Україна, м. Тернопіль

Інформаційні системи та електронні реєстри сьогодні відіграють ключову роль у діяльності органів державної влади та місцевого самоврядування, оскільки забезпечують ефективний збір, обробку, зберігання та обмін даними. Вони підвищують прозорість управління, мінімізують ризики допущення помилок і зловживань, а також сприяють оперативному прийняттю обґрунтованих управлінських рішень. Завдяки електронним системам та реєстрам державні послуги надаються швидше й зручніше, що підвищує довіру громадян та якість взаємодії між державою, бізнесом і суспільством. Інформаційні системи також підтримують аналітику, моніторинг і контроль у різних сферах публічного управління, забезпечуючи цілісність і доступність актуальної інформації [6, с. 37].

Пенсійний фонд України сьогодні виступає однією з найбільш інформаційно насичених державних установ, яка акумулює великі обсяги персональних даних громадян: відомості про трудову діяльність, доходи, соціальні виплати та іншу важливу інформацію. В умовах зростання глобальних кіберзагроз, дії воєнного стану та постійних спроб несанкціонованого втручання в систему інформаційних ресурсів, забезпечення конфіденційності й цілісності даних є одним із ключових пріоритетів у діяльності Фонду.

Діяльність органів Пенсійного фонду у сфері захисту інформації регулюється низкою законодавчих та підзаконних актів. Основними серед них є: Закони України «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні довірчі послуги», підзаконні акти Кабінету Міністрів України та Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ), що визначають порядок організації комплексної системи захисту інформації (КСЗІ).

Інформаційні ресурси Пенсійного фонду України становлять основу для здійснення пенсійних і страхових виплат, нарахування різноманітних видів соціальної допомоги, субсидій та пільг на оплату житлово-комунальних послуг. Вони забезпечують функціонування електронних реєстрів застрахованих осіб, контроль за сплатою єдиного соціального внеску та реалізацію державної політики у сфері соціального захисту населення [4, п.3]. Будь-яка втрата, спотворення чи несанкціоноване розголошення цих даних може мати серйозні соціально-економічні наслідки: порушення прав громадян на своєчасне отримання пенсій і соціальних виплат, появу шахрайських схем із використанням персональної інформації, створення загроз національній безпеці в системі соціального захисту, а також зниження рівня довіри населення до органів державної влади [1]. Тому, забезпечення надійного захисту інформації є для органів Пенсійного фонду не лише технічним завданням, а й важливим соціально-політичним пріоритетом.

У Головному управлінні Пенсійного фонду України в Тернопільській області функції з кіберзахисту, безпеки інформаційних систем та охорони електронних реєстрів

покладено на управління інформаційних систем та електронних реєстрів [5]. Усі інформаційні системи Пенсійного фонду, які містять персональні дані, проходять ретельну перевірку на відповідність встановленим вимогам із захисту інформації [2, ст. 9]. Це забезпечує юридичну основу для впровадження сучасних технічних і організаційних заходів безпеки.

Незважаючи на підвищену увагу до питань інформаційної безпеки, органи Пенсійного фонду України продовжують зіштовхуватися з низкою серйозних викликів. Серед них – зростання кількості кібератак, спрямованих на державні інформаційні ресурси; вплив людського фактора, оскільки частина витоків даних трапляється через необережність або недбалість працівників; ускладнення умов діяльності в умовах воєнного стану, коли окремі елементи інфраструктури зазнають ризику фізичного знищення чи кібератак з боку держави-агресора.

Технічна складова кіберзахисту має включати використання сучасних засобів антивірусного захисту, систем виявлення та запобігання проникнення, регулярне оновлення програмного забезпечення, резервне копіювання даних і шифрування інформаційних потоків. Важливо забезпечити постійний моніторинг роботи інформаційних систем для виявлення та нейтралізації потенційних загроз.

Окреме значення має підготовка персоналу. Працівники органів Пенсійного фонду повинні проходити регулярні тренінги з кібергігієни та відповідального поводження з інформацією, адже людський фактор є однією з головних причин витоку інформації. Також необхідно використовувати багаторівневу систему автентифікації користувачів і контролювати доступ до персональних відомостей лише в межах службових обов'язків.

Таким чином, ефективний захист інформації, яка міститься в інформаційних системах та електронних реєстрах держави, у тому числі і в органах Пенсійного фонду, має здійснюватися на основі комплексного підходу, який поєднує правові норми, технічні засоби безпеки та підвищення цифрової культури публічних службовців. Це дозволить забезпечити конфіденційність, цілісність і доступність даних, що є запорукою довіри громадян до державних інституцій.

Подальший розвиток безпеки та захист інформації, яка міститься в інформаційних ресурсах держави, у тому числі і Пенсійного фонду, повинен передбачати:

- перехід до хмарних технологій з високим рівнем захисту;
- впровадження системи багатофакторної автентифікації для працівників і користувачів електронних послуг;
- посилення міжвідомчої співпраці з ДССЗЗІ, Національним центром кіберзахисту, кіберполіцією та іншими структурами;
- підвищення рівня кіберграмотності працівників і користувачів електронних сервісів;
- прийняття Державної цільової програми кіберзахисту України [3].

Отже, захист інформації, що зберігається в інформаційних системах та електронних реєстрах органів влади в Україні, є комплексним завданням, яке охоплює правові, організаційні, технічні й криптографічні складові. Ефективне виконання цього завдання сприятиме не лише збереженню конфіденційності персональних даних громадян, а й підвищенню рівня довіри суспільства до державних інституцій, забезпеченню безперервності соціальних виплат і зміцненню національної безпеки. В умовах посилення кіберзагроз та викликів воєнного часу держава повинна постійно інвестувати в сферу інформаційної безпеки, удосконалювати технічні механізми захисту та підвищувати кваліфікацію працівників, відповідальних за безпечне функціонування інформаційних систем.

Список використаних джерел:

1. Задерейко О. Г., Трофименко О. Г., Єленич С. І., Гура В. І. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. URL: https://dspace.onua.edu.ua/items/73691819-8a0b-474c-b646-041a338a9299
2. Закон України Про захист інформації в інформаційно-комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
3. Петров С. Г. Захист державних електронних інформаційних ресурсів України. URL: http://jnas.nbuv.gov.ua/uk/article/UJRN-0001169823
4. Положення про Пенсійний фонд України. URL: https://www.pfu.gov.ua/2148251-polozhennya-pro-pensijnyj-fond-ukrayiny/
5. Положення про управління інформаційних систем та електронних реєстрів ГУ ПФУ в Тернопільській області. URL: https://www.pfu.gov.ua/tr/
6. Попов М., Комаровський І., Яценко В. Інформаційні системи та технології в публічному управлінні. URL: http://taais.oridu.odessa.ua/article/view/294963