ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2019.4(46)
Issue 4(46) 2019

УДК 342.9

Литвин Наталія Анатоліївна,
доктор юридичних наук, доцент,
старший науковий співробітник,
професор кафедри адміністративного
права і процесу та митної безпеки,
Університет державної фіскальної служби України,
м. Ірпінь, Україна

НАПРЯМИ ПІДВИЩЕННЯ РІВНЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ПОДАТКОВОЇ СЛУЖБИ УКРАЇНИ

У статті досліджено напрями підвищення рівня правового забезпечення інформаційної діяльності органів Державної податкової служби України. Визначено основні завдання системи правового забезпечення інформаційної діяльності органів ДПС України, зокрема: виявлення дестабілізуючих факторів та інформаційних загроз інтересам фіскальних органів та їх усунення; здійснення заходів щодо попередження правопорушень у сфері інформаційної діяльності фіскальних органів, забезпечення захисту їх інформаційної діяльності та захисту конфіденційної інформації щодо платників податків; зниження витрат на діяльність органів ДПС України; спрощення системи адміністрування податків і зборів.

Ключові слова: *інформація, інформаційна діяльність, правове забезпечення, державні органи, органи Державної податкової служби України.*

Правове забезпечення інформаційної діяльності органів Державної податкової служби України (далі – ДПС України), незважаючи на обмежене фінансування, здійснюється в межах державної системи захисту інформації та інформаційної діяльності в органах державної влади, і можуть бути представлені у вигляді комплексної самодостатньої системи. Тому визначення поточного стану та перспектив підвищення рівня правового забезпечення інформаційної діяльності органів ДПС України є важливим напрямом сучасної науки адміністративного та інформаційного права.

У науковій літературі окремі проблемні питання інформаційного забезпечення органів державної влади досліджували так вчені, як: І.В. Арістова, О.А. Баранов, К.І. Бєляков, І.Р. Березовська, В.М. Брижко, Б.А. Кормич, А.І. Марущак, А.М. Новицький, О.В. Олійник, І.М. Сопілко, М.Я. Швець, В.С. Цимбалюк та ін.

Метою цієї статті є визначення напрямів підвищення рівня правового забезпечення інформаційної діяльності органів ДПС України.

Система правового забезпечення та захисту інформаційної діяльності органів ДПС України, у функціональному сенсі, є рівноправною державній системі захисту

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).19

інформації, з тією лише різницею, що вона реалізує завдання цієї системи в межах власної діяльності. Основними завданнями системи правового забезпечення інформаційної діяльності органів ДПС України є:

– виявлення дестабілізуючих факторів та інформаційних загроз інтересам фіскальних органів та їх усунення;

– здійснення заходів щодо попередження правопорушень у сфері інформаційної діяльності фіскальних органів, забезпечення захисту їх інформаційної діяльності та захисту конфіденційної інформації щодо платників податків зокрема;

– зниження витрат на діяльність органів ДПС України;

– спрощення системи адміністрування податків і зборів.

Такі завдання пов'язані з вирішенням науково-технічних питань та питань, що належать до сфери правового регулювання інформаційної діяльності органів ДПС України. Відповідно серед напрямів правового забезпечення та захисту інформаційної діяльності органів ДПС України можна виокремити:

1) правовий (може бути представлений у вигляді двох складових: організаційно-правової та виконавчо-правової);

2) організаційний;

3) інженерно-технічний.

1. Правовий напрям полягає у розробці та реалізації законів, підзаконних правових актів, норми яких спрямовані на забезпечення та захист інформаційної діяльності органів ДПС України. При цьому необхідно зазначити, що якісне вдосконалення законодавства, яке регулює інформаційну діяльність органів ДПС України, може бути досягнуто за рахунок використання у практичній діяльності загальної аналітичної моделі при підготовці проекту нормативно-правового акта. Ця модель повинна містити наступні елементи:

– визначення проблеми, яку необхідно вирішити за допомогою нового нормативно-правового акта;

– визначення безпосередньої мети, очікуваних результатів;

– оцінка поточного законодавства, яке регулює інформаційну діяльність органів ДПС України, виявлення його недоліків;

– різні альтернативні варіанти вирішення проблеми, включаючи не законодавчі інструменти;

– вивчення наслідків, включаючи можливі результати (як позитивні, так і негативні), аналіз вигод і витрат;

– вибір напрямів реалізації проекту нормативно-правового акта на практиці на основі адміністративних, інформаційних або інших засобів, які забезпечують реалізацію акта;

– перелік установ і осіб для проведення консультацій та обговорення проекту нормативно-правового акта.

2. Наступним є організаційний напрям, зміст якого полягає в регламентації службової діяльності та взаємовідносин співробітників податкових органів, спрямованій на забезпечення та захист інформаційної діяльності в цих органах.

Організаційний напрям пов'язаний з охороною та забезпеченням режиму секретності в службових приміщеннях податкових органів, встановленням процедур використання технічних засобів захисту податкової інформації, роботою з кадрами,

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).19

документами, інформаційно-аналітичною діяльністю з виявлення різних загроз, об'єктом яких є інформаційна діяльність органів ДПС України. Цей напрям зумовлюється необхідністю здійснювати різні організаційні заходи, частина з яких регламентуються правовими актами, що встановлюють вимоги до збору, обробки, накопичення та зберігання інформації. До організаційних заходів належать:

– вибір місця розташування інформаційних, комп'ютерних та інформаційно-обчислювальних центрів;

– охорона зазначених центрів та центрів обробки, шифрування, передача і зберігання інформації;

– ретельний добір персоналу і постійний контроль за його переміщенням по території організації;

– виключення випадків повномасштабного ведення особливо важливих і секретних інформаційних робіт лише одним співробітником;

– створення служби адміністратора системної безпеки;

– організація служби парольного захисту;

– періодична зміна повноважень співробітників щодо інформації з обмеженим доступом;

– контроль доступу до електронних документів та інформації про них у частині, що стосується виконання службових обов'язків співробітників;

– контроль цілісності й авторизації програмного та інформаційного забезпечення автоматизованих систем обробки електронних документів;

– формування індивідуальних унікальних ідентифікаторів електронних документів та ідентифікаторів осіб, які безпосередньо беруть участь у їх введенні, обробці та передачі по мережах;

– ідентифікація абонентів телекомунікаційної мережі при вході в автоматизовану систему;

– реєстрація дій користувачів у спеціальному електронному журналі, доступному лише адміністратору інформаційної безпеки;

– наявність плану відновлення працездатності комп'ютерних, інформаційних та обчислювальних центрів після виходу їх з ладу;

– організація обслуговування центрів комп'ютерної інформації лише своїми силами й особами, які не зацікавлені у приховуванні фактів порушення роботи центру;

– універсальність засобів захисту від усіх користувачів (включаючи вище керівництво);

– покладання відповідальності на осіб, які мають забезпечити безпеку інформаційних центрів [1, с. 70–71].

Організаційні заходи сприяють створенню надійного механізму захисту податкової інформації, оскільки специфіка діяльності органів ДПС України менш стійка до дій не технічно-розвідувальних, а агентурних. Тобто загроза проникнення в інформаційну діяльність податкових органів походить, здебільшого, з боку користувачів або персоналу, відповідального за питання захисту інформації в цих органах. Потрібно посилювати внутрішню безпеку в органах ДПС України, ретельно добирати персонал, особливо той, який виконує обов'язки адміністратора

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).19

інформаційних систем, а не користувача, і має необмежений доступ до баз даних. Така проблема ускладнюється тим, що адміністратор, по суті, є особою, яка контролює дії користувачів, завдяки програмним засобам він може бачити, які дії здійснював користувач (копіював, видаляв, відправляв, отримував тощо), яку інформацію запрошував. При цьому сам адміністратор може змінювати ці відомості, володіючи відповідними навичками. Контроль же за адміністраторами мінімальний. Правопорушникам досить знайти важелі впливу на адміністратора – і безпека інформаційної діяльності органу ДПС України втратить свою цілісність. Крім цього, небезпечним є не лише сам факт отримання правопорушниками інформації, а й відсутність його фіксації. Тобто про правопорушення нікому не буде відомо, допоки правопорушники не скористаються інформацією у своїх цілях, і сам факт наявності у них такої інформації не буде свідчити про вчинене правопорушення.

Загалом організаційні заходи в органах ДПС України можуть бути спрямовані на вирішення таких комплексних завдань:

– організація режиму (пропускного, всередині об'єкта) та охорони з метою унеможливлення таємного проникнення на територію органу ДПС України і в режимні приміщення установи сторонніх осіб;

– добір, вивчення і розстановка кадрів, навчання правилам роботи із захищеними відомостями, ознайомлення їх із заходами відповідальності за порушення правил захисту податкової інформації;

– організація використання технічних засобів збору, обробки, накопичення та зберігання податкової інформації, що захищається;

– організація роботи з аналізу внутрішніх і зовнішніх загроз податкової, що захищається, та вироблення заходів щодо забезпечення її захисту;

– організація контролю за роботою персоналу з податковою інформацією, що захищається, порядком обліку, зберігання та знищення документів і технічних носіїв.

3. Інженерно-технічний напрям полягає у використанні технічних та програмно-апаратних засобів, а також технічних систем для забезпечення та захисту інформаційної діяльності органів ДПС України. Інженерно-технічний напрям забезпечується:

– захистом від несанкціонованого доступу до системи шляхом встановлення спеціальних технічних систем електронної безпеки (наприклад, зовнішній імпульсний і хвильовий захист, файли-невидимки, програми-примари тощо);

– екрануванням кімнат, де знаходяться інформаційні засоби;

– резервуванням особливо важливих інформаційних підсистем;

– організацією інформаційних мереж із можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок;

– встановленням резервних систем електроживлення;

– встановленням обладнання виявлення і гасіння пожежі, виявлення та відкачування води;

– вжиттям конструктивних заходів захисту від розкрадань інформації, саботажу, диверсій, вибухів тощо;

– оснащенням приміщень замками та системами сигналізації;

– установкою фільтрів на джерела живлення;

– установкою генераторів поглинання шумів;

– застосуванням комп'ютерів, які відповідають певним технічним нормам з ефективного захисту інформації [1, с. 66–67].

Усі зазначені вище заходи ускладнюють можливість розкрадання, знищення або перехоплення інформації шляхом прийому побічного випромінювання, апаратних шумів засобів обчислювальної техніки, запису з ліній зв'язку при передачі між ЕОМ тощо. Незважаючи на це, перше, на що доцільно звернути увагу, – це на проблему загального низького рівня інженерно-технічного напряму правового забезпечення та захисту інформаційної діяльності в податкових органах. При цьому, якщо в центральних органах ДПС України інженерно-технічне забезпечення перебуває на пристойному рівні, то в органах, які знаходяться на периферії, його стан є незадовільним. Висока вартість технічних засобів є основним фактором, який не дозволяє повною мірою реалізувати увесь їх потенціал на практиці. Крім того, в органах ДПС України донині використовується підхід до фінансування за "залишковим" принципом. А у зв'язку з хронічним дефіцитом державного бюджету України позитивне вирішення цієї проблеми найближчим часом не передбачається.

Відзначимо, що без належного правового забезпечення використання засобів інженерно-технічного захисту буде неможливим, оскільки вони вимагають значних фінансових вкладень. Тобто, за відсутності правової складової, яка буде регламентувати необхідність виділення коштів на ті чи інші технічні та програмно-апаратні засоби, кошти виділені не будуть. Зазначене дозволяє зробити висновок про те, що всі напрями забезпечення і захисту інформаційної діяльності органів ДПС України повинні застосовуватися на практиці комплексно.

Наголосимо, що проблемою, з якою стикаються органи ДПС України, є відсутність на ринку вітчизняних розробок і пристроїв, які можуть перешкоджати несанкціонованому проникненню в приміщення, що охороняється. Ті ж пристрої, представлені на ринку, можуть містити в собі вже встановлені "закладки", при цьому ці "закладки" можуть бути конструктивними елементами таких пристроїв, що робить неможливою їх ідентифікацію як "закладок". У цьому випадку ми пропонуємо державі подбати про безпеку своїх органів, шукати резерви і вкладати гроші в розробку українських засобів захисту.

Зважаючи на важливість роботи державних органів, вбачається, що в довгостроковій перспективі держава має подбати про те, щоби все основне програмне забезпечення, системи контролю доступу були українського виробництва. Так, це величезні фінансові витрати, але втрати, які вже понесла і може понести Україна у зв'язку з порушенням інформаційної діяльності державних органів, обчислюються десятками мільярдів доларів. При цьому державі для розробки таких пристроїв і програм необхідно залучити вітчизняних виробників.

Програмні засоби – це сукупність програм, які забезпечують розмежування доступу до податкової та митної інформації й унеможливлення несанкціонованого використання цієї інформації сторонніми особами. Такий засіб включає різноманітні програми, програмні комплекси та програмні системи захисту, пов'язані з ідентифікацією користувачів, контролем систем захисту, доступу до інформації тощо. Програмним засобом забезпечується захист інформаційної мережі податкового органу і від зараження комп'ютерними вірусами. Існує група антивірусних

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).19

засобів, які можуть забезпечити надійний захист комп'ютера. Серед найбільш відомих і використовуваних у державних органах України слід виділити антивірусні програми: Avast! (Чехія), Agnitum (Росія), Doctor Web (Росія), ESET (Словаччина), Kaspersky (Росія). Головний мінус цих програм полягає в тому, що їх функціонування споживає величезну кількість системних ресурсів. А враховуючи наявність у більшості податкових органів старої техніки, це викликає постійні збої в роботі комп'ютерів, їх зависання, що у підсумку призводить до гальмування робочого процесу. Таким чином, основна проблема, яка стоїть перед програмним засобом забезпечення захисту інформаційної мережі фіскального органу, – це отримання максимального захисту за мінімального використання системних ресурсів [2, с. 168]. У зв'язку з обмеженими можливостями системних ресурсів більшості периферійних органів ДПС України, програмні засоби в їх діяльності використовуються в основному з метою розмежування доступу користувачів до масиву податкової та митної інформації, незважаючи на те, що вони повинні оберігати інформаційну систему від атак на неї, які можна поділити на:

– локальні атаки;
– віддалені атаки;
– атаки на потоки даних.

Дії порушника, який, маючи фізичний доступ до комп'ютера, робочої станції або сервера, що знаходиться всередині цієї системи, намагається отримати доступ до інформаційної системи органу ДПС України та даних, які в ній зберігаються, будуть кваліфіковані як локальна атака. Локальні атаки характерні для внутрішніх навмисних загроз і найчастіше їх здійснюють співробітники податкових органів. До них відносяться: соціальна інженерія; закладки в програмному забезпеченні; подолання обмежень на рівні програмно-апаратних засобів; отримання доступу на етапі завантаження операційної системи; атака на засоби аутентифікації; підвищення привілеїв; стороннє програмне забезпечення тощо.

Якщо ж порушник намагається отримати доступ до інформаційної системи органу ДПС України через віддалений комп'ютер, не пов'язаний з інформаційною системою цього органу, то такі атаки класифікуються як віддалені. Дистанційні атаки характерні для зовнішніх навмисних загроз. До них відносяться: збір інформації про об'єкт захисту; атаки на маршрутизацію; атаки на конкретні сервіси; переповнення буфера тощо.

Якщо порушник здійснює атаку на мережевий вузол, який бере участь в обміні інформацією між кількома комп'ютерами, то така атака кваліфікується як атака на потоки даних. Атаки на потоки даних характерні як для внутрішніх навмисних загроз, так і зовнішніх. До них відносяться: атака повтором, атака підміною, атаки на основі мережевої маршрутизації, перехоплення сесії тощо.

Обговорюючи проблемні питання правового забезпечення й захисту інформаційної діяльності органів ДПС України, необхідно відзначити проблему, що полягає у слабкому технічному оснащенні окремих підрозділів органів ДПС України та несумісності програмного забезпечення, що призводить до різного роду збоїв при виконанні доручень та завдань керівництва. Вирішення проблем цього напряму безпосередньо пов'язане з необхідністю використання сучасних технічних та апаратно-програмних засобів збору, накопичення, обробки та передачі

інформації. Одним із шляхів інформаційно-технологічного забезпечення, разом із технологією Blockchain, вбачається необхідність переведення органів ДПС України на Open Sorce-рішення. Упродовж останніх років корпорація Microsoft вимагає від України оплати в розмірі мільярдів гривень за використання її програмних продуктів без ліцензії. Претензія обґрунтована, але ніякого сенсу в закупівлі платного програмного забезпечення на таку суму немає: увесь документообіг у державних органах влади, у тому числі і в органах ДПС України, можна перевести на Open Sorce-рішення (безкоштовні програми). Так, на виставці CeBIT-2014 було продемонстровано з десяток альтернатив MS Office, а також конструкторів систем електронного обігу для державного сектора. Причому робота в них здійснюється через веб-інтерфейс: не потрібно навіть установки на комп'ютер, а його потужність не має значення. Тоді між собою будуть конкурувати не компанії, а проектні групи, і монополізація ринку буде усунена [3].

Криптографічними засобами інженерно-технічного захисту інформаційної діяльності органів ДПС України є засоби шифрування, кодування чи іншого перетворення податкової інформації, що зберігається й обробляється в електронному вигляді, передається за допомогою систем та мереж зв'язку. По суті, криптографічні засоби захищають електронний документообіг органів ДПС України.

Криптографічний засіб захисту є одним із найнадійніших, оскільки охороні підлягає інформація у вигляді файлу, а не фізичний носій, на якому інформація знаходиться. Цей засіб захисту реалізується в усіх програмах, які дозволяють надсилати податкову звітність в електронному вигляді. Основні напрями використання криптографічних засобів – передача конфіденційної інформації по каналах зв'язку (електронна пошта), встановлення достовірності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді. При цьому до переваг криптографічних засобів автор відносить забезпечення високої гарантованої стійкості захисту, який можна розрахувати і виразити в числовій формі (середнім числом операцій або часом, необхідним для розкриття зашифрованої інформації чи обчислення ключів); а до недоліків – значні витрати ресурсів (часу, продуктивності процесорів) на виконання криптографічних перетворень інформації; труднощі спільного використання зашифрованої (підписаної) інформації, пов'язані з управлінням ключами (генерація, розподіл тощо); високі вимоги до збереження особистих ключів і захисту відкритих ключів платників податків від підміни [2, с. 171, 172].

Відзначимо, що потенціал інженерно-технічного напряму забезпечення і захисту інформаційної діяльності органів ДПС України ще повністю не розкритий, оскільки для цього потрібне комплексне фінансування. Але доцільно враховувати той факт, що застосування одних лише засобів захисту з інженерно-технічного напряму може дати ефективний результат тільки при роботі окремого комп'ютера або комп'ютерів, що функціонують в ізольованій локальній мережі при організації введення даних вручну та обмеженні доступу до локальної мережі організаційними заходами.

Отже, будь-яка сфера державного управління забезпечується ефективною діяльністю кожної складової її державно-правового механізму, що складається із системи взаємопов'язаних і взаємоузгоджених державно-правових інституцій.

DOI (Article): https: //doi.org/10.36486/np.2019.4(46).19

Завданнями таких інституцій є створення умов для успішного забезпечення інформаційної діяльності та безпеки як центральних органів влади, так і органів ДПС України. Для вирішення в умовах сьогодення окреслених вище напрямів правового забезпечення інформаційної діяльності та безпеки ДПС України потрібен не лише час та суттєві інвестиції, а й політична воля керівництва держави та керівників ДПС України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Лазарев А.Ю.* Правовое обеспечение защиты информации при использовании электронного документооборота в арбитражном судопроизводстве: дис. ... канд. юрид. наук: 05.13.19. Москва, 2007. 204 с.

2. *Гордійчук М.В.* Правове регулювання електронного документообігу в сфері оподаткування*:* дис. ... канд. юрид. наук: 12.00.07. Ірпінь, 2017. 248 с.

3. Переход Правительства на электронное управление быстро искоренит коррупцию в стране. Дата оновлення: 17.03.2014. URL: http://aeaep.com.ua/perohod-pravy-tel-stva-na-e-lektronnoe-upravleny-e-y-skoreny-t-korruptsy-yu-v-strane/ (дата звернення: 05.09.2019).

REFERENCES

1. *Lazariev A.Yu.* (2007) Pravovoye obespechenie zashchity informatsii pri ispolzovanii elektronnoho dokumentooborota v arbitrazhnom sudoproizvodstve. “Legal security of information protection in the use of electronic document flow in arbitration proceedings”: diss. PhD in Law: 05.13.19. Moscow. 204 p. [in Russian].

2. *Hordiichuk M.V.* (2017) Pravove rehuliuvannia elektronnoho dokumentoobihu v sferi opodatkuvannia. “Legal regulation of electronic document flow in the sphere of taxation”: dis ... PhD in Law: 12.00.07. Irpin. 248 p. [in Ukrainian].

3. Perekhod Pravitelstva na elektronnoie upravlenie bystro iskorenit korruptsiu v strane. “The Government’s transition to e-government will quickly eradicate corruption in the country”. Date of approval: 17.03.2014. URL: http://aeaep.com.ua/perohod-pravy-tel-stva-na-e-lektronnoe-upravleny-e-y-skoreny-t-korruptsy-yu-v-strane/ (date of application: 05.09.2019) [in Russian].

UDC 342.9

Lytvyn Nataliia,
Doctor of Juridical Sciences, Docent, Senior Research Associate,
Professor at the Department, State Fiscal Service of Ukraine,
Irpin, Ukraine

DIRECTIONS OF INCREASING THE LEVEL OF LEGAL SUPPORT OF INFORMATION ACTIVITIES OF THE STATE TAX SERVICE OF UKRAINE

The article investigates the directions of increasing the level of legal support of information activity of the departments of the State Tax Service of Ukraine. The main tasks of the system of legal support of information activity of the departments of the State Tax Service of Ukraine are determined, in particular: identification of destabilizing factors and information threats to the interests of the fiscal departments and their elimination; implementation of measures for prevention of offenses in the sphere of information activity of fiscal departments, ensuring protection of their information

activity and protection of confidential information concerning taxpayers in particular; reduction of expenditures for the activity of the State Tax Service of Ukraine simplify the system of administration of taxes and fees.

The directions of improvement of administrative-legal providing of information activities of the authorities of the State Tax Service of Ukraine are offered, namely: legal (it can be presented in the form of two components: organizational-legal and executive-legal); organizational; technical. The legal direction consists in development and implementation of laws, subordinate legal acts, which norms are aimed at providing and protection of information activities of the authorities of the State Tax Service of Ukraine. The organizational direction provides the regulation of official activities and relationship of the staff of tax and customs authorities which is aimed at providing and protection of information activities in these authorities. The technical direction consists in the use of technical and software-hardware tools and also technical systems for providing and protection of information activities of the authorities of the State Tax Service of Ukraine.

It is concluded that any sphere of public administration is ensured by the effective activity of each component of its state-legal mechanism, consisting of a system of interrelated and mutually agreed state-legal institutions. The tasks of such institutions are to create the conditions for successful provision of information activity and security of both central and state police departments of Ukraine. In order to decide in the current areas of legal support for information activities and security of the State Tax Service of Ukraine, not only time and substantial investments, but also the political will of the government of the state and the leaders of the State Security Service of Ukraine are required.

Keywords: information, information activity, legal support, state bodies, bodies of the State Tax Service of Ukraine.

Отримано: 26.09.2019