**ДЕРЖАВНА ФІСКАЛЬНА СЛУЖБА УКРАЇНИ**
**УНІВЕРСИТЕТ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ**

**На правах рукопису**

**ШАПКА АЛЬОНА ВОЛОДИМИРІВНА**

УДК 342.9: (477)

# АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

12.00.07 – адміністративне право і процес, фінансове право, інформаційне право

Дисертація на здобуття наукового ступеня
кандидата юридичних наук

Науковий керівник:
кандидат юридичних наук,
старший науковий співробітник
**Литвин Наталія Анатоліївна**

**Ірпінь – 2016**

# ЗМІСТ

# ВСТУП

**Актуальність теми.** На сучасному етапі розвитку України як економічно розвиненої та правової держави особливе місце займає національна безпека, важливою складовою якої є інформаційна. Держава, яка має розвинені інформаційні системи та засоби інформаційного захисту, є лідером в економічній, політичній та соціальній сферах, має стратегічну і тактичну переваги, зокрема у передових інформаційних технологіях.

Державна фіскальна служба України (далі – ДФС України) на сьогодні є одним з найважливіших органів системи державного управління, який реалізує державну політику у податковій та митній сферах. Ефективне функціонування зазначених сфер є необхідною умовою захисту економічних інтересів України.

Для розвитку та покращення діяльності органів ДФС України у сфері захисту інформації було затверджено Стратегічний план розвитку ДФС України на 2015–2018 рр., у якому одним із пріоритетів визначено впровадження новітніх інформаційних технологій, спрямованих на охорону державної таємниці, технічного та криптографічного захисту інформації в апараті ДФС України та її територіальних органах.

На сьогодні правопорушення в економічній сфері вчиняються з використанням різноманітних схем протиправної діяльності, у тому числі через незаконне заволодіння інформацією та проникнення в державні інформаційні системи. У зв’язку з цим питання забезпечення інформаційної безпеки в діяльності органів ДФС України та її нормативно-правове регулювання залишаються актуальними, оскільки з розвитком інформаційних відносин у ДФС України виникає загроза несанкціонованого розголошення інформації з обмеженим доступом, незаконного втручання до інформаційних систем, що становить загрозу зміни інформації та порушення встановленого порядку її маршрутизації. Отримавши таку інформацію,

зловмисники мають можливість використовувати її для вчинення інших протиправних дій, зокрема ухилення від сплати податків, зборів тощо.

Незважаючи на наукову і практичну цінність питань, пов'язаних із забезпеченням інформаційної безпеки в діяльності ДФС України, донині немає єдиного підходу щодо виокремлення заходів забезпечення інформаційної безпеки в органах ДФС України. Унаслідок цього, системне дослідження вказаних проблем набуває додаткової актуальності.

Основне теоретичне підґрунтя дослідження у сфері інформаційного права становлять праці таких відомих українських вчених, як І.В. Арістова, К.І. Беляков, В.М Брижко, А.І. Берлач, В.О. Глушков, В.Д. Гавловський, Б.А. Кормич, Р.А. Калюжний, О.В. Логінов, В.М. Росоловський, А.М. Новицький, Н.Б. Новицька, О.В. Олійник, С.П. Ріппа, М.Я. Швець та інші. Проблеми формування інформаційної безпеки, її правового регулювання досліджували такі науковці, як І.Р. Березовська, А.І. Брезвін, В.Т. Білоус, О.А. Долгий, Л.М. Касьяненко, Т.С. Касянюк, О.О. Косиця, Г.М. Линник, Н.А. Литвин, В.Я. Мацюк, О.В. Олійник, В.М. Попович, О.П. Рябченко, І.С. Стаценко-Сургучова, Д.Я. Семир'янов, В.І. Теремецький, В.С. Цимбалюк, В.О. Шамрай, В.К. Шкарупа, Ф.О. Ярошенко та іншими.

Серед дисертаційних досліджень необхідно виокремити роботу Линника Г.М., який здійснив загальну характеристику адміністративно-правового регулювання інформаційної безпеки України, розглянув інформаційну безпеку держави, як діяльність суб'єктів права щодо задоволення національних інтересів в інформаційній сфері шляхом управління реальними чи потенційними загрозами. Березовська І.Р. розглянула історичні етапи розвитку адміністративно-правових засобів забезпечення інформаційної безпеки України, з'ясувала особливості застосування дозвільних і реєстраційних засобів забезпечення інформаційної безпеки в діяльності органів державної влади України. Олійник О.В. ґрунтовно розглянув основоположні принципи формування інформаційної безпеки держави, напрями її правового регулювання.

Вивченню окремих питань інформаційної безпеки в діяльності органів ДПС України було присвячено дисертаційну роботу Субіної Т.В. «Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України» (Ірпінь, 2010). На відміну від вказаної роботи, нами зосереджено увагу на удосконаленні наукових теоретичних підходів до застосування заходів забезпечення інформаційної безпеки в діяльності органів ДФС України, визначення сутності управління інформацією в діяльності органів ДФС України та обґрунтування напрямів удосконалення національного законодавства і практики його застосування у зазначеній сфері.

Віддаючи належне результатам попередніх наукових досліджень з цієї проблематики, необхідно зазначити, що в умовах реформування ДФС України питання інформаційної безпеки не отримали належного висвітлення і тому потребують додаткового наукового обґрунтування. Наведене не лише зумовило вибір теми дисертаційного дослідження, а й свідчить про актуальність її наукових положень як для теоретичного аналізу забезпечення інформаційної безпеки в діяльності органів ДФС України, так і для визначення нових концептуальних підходів щодо їх удосконалення.

**Зв'язок роботи з науковими програмами, планами, темами.** Обраний напрям дослідження пов'язаний із втіленням в життя окремих положень Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V та Стратегічного плану розвитку ДФС України на 2015–2018 роки, затвердженого Наказом ДФС України від 12.02.2015 № 80. Дисертацію виконано відповідно до «Стратегії національної безпеки України», затвердженої Указом Президента України від 26.05.2015 № 287/2015, та «Пріоритетних напрямів розвитку правової науки на 2011–2015 рр.», затверджених постановою Загальних зборів НАПрН України 24 вересня 2010 року. Відповідне наукове завдання, яке визначає характер досліджуваної проблематики, закріплено у планах науково-дослідної роботи кафедри

управління, адміністративного права і процесу та адміністративної діяльності Національного університету державної податкової служби України – «Правове регулювання управлінської та правоохоронної діяльності у сфері оподаткування» (державний реєстраційний номер УкрНТІ 0112U001826).

Тема дисертаційного дослідження затверджена Вченою радою Національного університету ДПС України від 24 квітня 2014 року (протокол № 8), розглянута координаційним бюро відповідного відділення Національної академії правових наук України і має позитивний відгук щодо актуальності, коректності формулювання та доцільності дослідження у вигляді дисертації за спеціальністю 12.00.07.

**Мета і завдання дослідження.** Мета роботи полягає в тому, щоб на підставі проведеного аналізу наукової літератури, чинних нормативно-правових актів, досвіду зарубіжних країн та правозастосовної практики уповноважених органів удосконалити теоретичні основи і практику адміністративно-правового забезпечення інформаційної безпеки в діяльності органів ДФС України.

Для досягнення зазначеної мети були сформовані основні завдання:

– визначити поняття та суть інформації, яку використовують органи ДФС України для реалізації покладених на них функцій та завдань;

– сформувати розуміння інформаційної безпеки в органах ДФС України для своєчасного виявлення загроз, які виникають у податковій та митній сферах;

– встановити коло суб’єктів, які забезпечують інформаційну безпеку в органах ДФС України;

– проаналізувати інформаційні ресурси, які використовують органи ДФС України у своїй діяльності;

– виокремити напрями вдосконалення інформаційного забезпечення управління в органах ДФС України;

– здійснити аналіз інформаційних відносин та визначити заходи щодо організації захисту інформації в органах ДФС України;

– з’ясувати питання адміністративної відповідальності, пов’язані із забезпеченням інформаційної безпеки органів ДФС України;

– сформувати пропозиції та рекомендації до чинного законодавства, що стосуються інформаційної безпеки в діяльності органів ДФС України;

– узагальнити позитивний досвід зарубіжних країн щодо використання правових засад забезпечення інформаційної безпеки в органах ДФС України.

*Об’єктом дослідження* є суспільні відносини, які виникають та реалізуються в процесі забезпечення інформаційної безпеки органів Державної фіскальної служби України.

*Предметом дослідження* є адміністративно-правові засади забезпечення інформаційної безпеки в діяльності органів ДФС України.

*Методи дослідження.* Для реалізації поставленої мети та вирішення сформованих завдань у дисертаційній роботі використано комплекс дослідницьких загальнонаукових і спеціальних методів наукового пізнання з урахуванням специфіки актуальної проблематики забезпечення інформаційної безпеки в діяльності органів ДФС України.

Основою дослідження став діалектичний метод пізнання, який дозволив розглянути проблеми у дисертації, як єдність їх соціального змісту та юридичної форми (підрозділи 1.1, 2.1, 2.3). За допомогою поширення отриманих висновків і знань та логіко-семантичного способів було деталізовано сутність таких понять, як: «податкова інформація», «митна інформація», «інформаційна безпека в діяльності органів ДФС України», «управління інформаційними ресурсами органів ДФС України», «інформаційне правопорушення у діяльності ДФС України», «адміністративна відповідальність за вчинені інформаційні правопорушення», «податкова таємниця», «митна таємниця» (підрозділи 1.1, 1.2, 2.2, 2.3, 2.4, 3.1). Застосування системного аналізу та порівняльно-правового методу дозволило розглянути методичні підходи до використання вітчизняного та зарубіжного досвіду у сфері реалізації адміністративно-правових засобів забезпечення інформаційної безпеки (підрозділ 3.2).

Використання різних способів аналізування, синтезування та створення класифікацій і групувань дало можливість визначити статус, завдання та функції суб'єктів, які забезпечують інформаційну безпеку у податковій і митній сферах держави (підрозділ 1.3). Порівняльно-правовий, організаційно-правовий, системно-функціональний та системно-структурний методи дозволили визначити поняття та відповідні ознаки інформаційної безпеки та інформаційного забезпечення управління в органах ДФС України (підрозділи 1.2, 2.1).

*Нормативно-правову основу дослідження* склали Конституція України, Податковий кодекс України, Митний кодекс України, закони України: «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про інформацію», «Про Концепцію Національної програми інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», окремі норми, що забезпечують інформаційну безпеку ДФС України, конвенції, угоди, які регулюють інформаційну безпеку, як суспільні відносини в інформаційному середовищі, законодавство зарубіжних країни (США, Великої Британії, Німеччини, Естонії, Канади, Франції, Нідерландів тощо).

*Емпіричною базою роботи* є узагальнення практичної діяльності органів ДФС України, довідникових видань, аналіз публікацій та обробка даних офіційних інформаційних джерел щодо забезпечення інформаційної безпеки органів державної влади, зокрема органів ДФС.

**Наукова новизна одержаних результатів.** Дисертація є одним із перших в Україні комплексним науковим дослідженням адміністративно-правового забезпечення інформаційної безпеки в діяльності органів Державної фіскальної служби України. За результатами дослідження внесено пропозиції до чинного законодавства у сфері формування інформаційної безпеки. На підставі проведеного дослідження сформульовано й обґрунтовано низку висновків, рекомендацій та пропозицій, зокрема:

*уперше:*

– дано визначення понять: «митна інформація, яку запропоновано розуміти як коло відомостей і даних, що збирають, накопичують та використовують органи ДФС для реалізації державної митної політики»;

«інформаційна безпека в діяльності органів ДФС України – це стан захисту інформації, інформаційних технологій та інформаційних ресурсів, працівників служби, фізичних та юридичних осіб від неправомірних дій чи бездіяльності суб'єктів інформаційних відносин, за якого здійснюється попередження, виявлення та протидія інформаційним правопорушенням»;

– обґрунтовано доцільність впровадження в діяльність ДФС України до інформаційної системи «Податковий блок» підсистеми «Електронний журнал безпеки» з метою контролю за діями користувачів для виявлення і протидії правопорушенням;

*удосконалено:*

– визначення понять: «управління інформаційними ресурсами органів ДФС України – це встановлена законодавством діяльність органів ДФС України щодо реалізації правових, організаційних, управлінських й технічних заходів, спрямована на належне отримання, накопичення, опрацювання, використання й зберігання інформації, необхідної для виконання покладених на ДФС функцій»;

«податкову таємницю запропоновано розуміти як сукупність інформації з обмеженим доступом, яка містить персональні дані фізичних та юридичних осіб, конфіденційну і службову інформацію, а також державну таємницю, яка стає відомою органам ДФС у зв'язку з виконанням покладених на них функцій і підлягає захисту»;

«митну таємницю запропоновано розглядати як сукупність інформації, що стає відомою органам ДФС під час реалізації державної митної справи і містить персональні дані фізичних та юридичних осіб, конфіденційну, службову інформацію, державну таємницю, використовується органами ДФС тільки для виконання митних завдань і підлягає захисту»;

– завдання та функції сучасної системи суб'єктів забезпечення інформаційної безпеки в діяльності органів ДФС України, а саме: Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації, Департаменту інформаційних технологій, Департаменту обслуговування платників, Департаменту моніторингу доходів та обліково-звітних систем, Головного управління внутрішньої безпеки;

*дістали подальшого розвитку:*

– напрями вдосконалення інформаційного забезпечення управління в органах ДФС України;

– наукові підходи щодо розуміння адміністративної відповідальності у сфері забезпечення інформаційної безпеки органів ДФС України, як важливого чинника організації захисту інформації в податковій та митній сферах;

– заходи вдосконалення захисту інформації в діяльності органів ДФС України (спеціальне діловодство; режим секретності, включаючи технічний захист інформації; технічний і криптографічний захист інформації; голографічний захист носіїв інформації; правовий та організаційний захист інформації, а також складові всіх інших видів (правову основу окремих різновидів захисту інформації);

– положення щодо недостатньої законодавчої урегульованості інституту податкової та митної таємниці, у зв'язку з чим обґрунтовано рекомендації щодо удосконалення діючого законодавства;

– пропозиції щодо запозичення позитивного досвіду у сфері інформаційної безпеки державних органів.

**Практичне значення одержаних результатів** полягає в тому, що узагальнення та висновки, які містяться в дисертації, можуть бути використані при проведенні подальших наукових досліджень з питань адміністративно-правового забезпечення інформаційної безпеки в діяльності органів ДФС України, у тому числі:

– *у науково-дослідній сфері* – як основа для подальшого розроблення загальнотеоретичних питань, які можуть бути пов’язані з удосконаленням адміністративно-правових заходів забезпечення інформаційної безпеки в діяльності органів ДФС України (акт про впровадження від 21 березня 2016 року);

– *у правотворчій сфері* – для удосконалення чинних і розроблення проектів нормативно-правових актів, спрямованих на гарантування інформаційної безпеки органів ДФС України;

– *у практичній діяльності* – з ціллю підвищити результативність організації інформаційного забезпечення органів ДФС України (акт про впровадження від 25 березня 2016 року);

– *у навчальному процесі* – протягом підготовки навчальних підручників, посібників, методичних матеріалів, які можуть бути основою для проведення лекцій, семінарів та практичних занять для таких навчальних дисциплін, як «Адміністративна діяльність контролюючих органів в сфері оподаткування», «Інформаційне право» (акт про впровадження від 18 березня 2016 року).

**Особистий внесок здобувача.** Положення, що розглянуто в науковій роботі та винесено на захист, є результатом самостійної праці автора дисертації. Наукові ідеї та розробки, які належать співавторам опублікованих праць, у дисертаційному дослідженні не використовувалися. Особистий внесок до опублікованих колективних наукових праць пропорційний кількості співавторів.

**Апробація результатів дослідження**. Основні положення, висновки і рекомендації, розроблені в процесі дослідження, обговорювались на розширеному засіданні кафедри адміністративного права і процесу та митної безпеки Університету державної фіскальної служби України. Окремі положення та результати роботи було оприлюднено на 8 міжнародних і науково-практичних конференціях, зокрема: «Проблеми впровадження інформаційних технологій в економіці» (Ірпінь, 23 січня – 30 березня 2012

року), «Проблеми гуманізації навчання та виховання у вищому закладі освіти» (Ірпінь, 29 – 30 березня 2012 року), «Стратегія і тактика правових реформ: виклики сучасності» (Київ, 5 березня 2013 року), «Административное право и процесс: история, современность, перспективы развития» (Москва-Запоріжжя, 21 – 22 травня 2014 року); «Реформування податкової системи України в контексті глобалізаційних викликів» (Ірпінь, 21 листопада 2014 року); «Проблеми правової реформи та розбудови громадянського суспільства в Україні» (м. Харків, 16 – 17 жовтня 2015 року); «Верховенство права та правова держава» (м. Ужгород, 16 – 17 жовтня 2015 року); «Юридичні науки: проблеми та перспективи» (м. Херсон, 20 – 21 травня 2016 року).

**Публікації.** Основні положення дисертації відображено у 14 публікаціях, серед яких 5 наукових статей опубліковано у наукових фахових виданнях України, 1 стаття в іноземному виданні, 8 тез наукових повідомлень на науково-практичних конференціях.

**Структура роботи**. Робота складається зі вступу, трьох розділів, дев’яти підрозділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 205 сторінок, список використаних джерел налічує 174 найменування.

# РОЗДІЛ 1

# ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

## 1.1. Поняття та сутність інформації в діяльності органів ДФС України

На сьогодні, враховуючи безупинний розвиток інформаційних технологій та появу інноваційних програмних забезпечень і компонентів, інформація стає ключовим елементом розвитку такого продукту. При цьому для продуктивного та виваженого розвитку зазначених технологій в економічній сфері держава повинна мати певні механізми реалізації інформаційної політики для ефективного використання такого потенціалу.

Глобалізація економіки у світі призвела до інтеграції різних ресурсних елементів, взаємопроникнення матеріальних та інформаційних складових економіки. Водночас, інформація дедалі більше відіграє головну роль у досягненні економічних, соціальних та політичних цілей життєдіяльності держави.

ДФС України є одним з найважливіших органів державної влади, який забезпечує реалізацію економічної політики нашої країни у податковій та митній сферах. У зв’язку з цим основним аспектом діяльності фіскальної служби є розвиток наявних та впровадження новітніх інформаційних технологій для належної систематизації та захисту інформації, яку використовують органи ДФС для виконання завдань та функцій. Цього можливо досягнути, поєднавши регулюючі та безпекові механізми.

Розглянемо більш детально законодавчі та наукові підходи дослідників до трактування поняття інформації.

У сучасному світі інформацію розглядають на одному рівні з матеріальними та енергетичними ресурсами і визначають, як важливий чинник якісних змін у житті суспільства [150, с. 127].

Інформацію широко використовують на всіх етапах розвитку суспільства, що пояснюється насамперед її різноаспектністю. На думку Субіної Т.В., основною сферою використання інформації мають бути органи державної влади. До таких органів належить ДФС України, яка є основним суб'єктом нашого дослідження [147, с. 22].

У процесі управління державою інформація відіграє важливу роль. Адже її збір, оброблення та систематизація дозволяють чітко визначити цілі та засоби досягнення поставленої мети. Розробка відповідних механізмів повинна включати в себе як механізми збору, зберігання інформації, так і механізми захисту від несанкціонованого втручання в інформаційні системи.

Велике значення також має оперативність та якість збирання і оброблення інформації. Визначають пряму залежність між швидкістю збирання, оброблення інформації та ефективністю прийнятих і реалізованих управлінських рішень. Тобто, чим більше опрацьовується інформації, тим більш тісними стають зв'язки між структурними підрозділами органів держаного управління та контролю і тим більш якісно та глибоко вони впливають на суспільство.

Інформацією, згідно закону України «Про інформацію», визнають будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [22].

У Цивільному кодексі України поняття «інформація» так само трактується, як і в Законі України «Про інформацію» [7].

Законом України «Про телекомунікації» інформація визначена, як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [28].

У свою чергу, у Законі України «Про захист економічної конкуренції» інформація розглядається, як відомості в будь-якій формі й вигляді та

збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їхніх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [30].

Як бачимо, на законодавчому рівні інформацію трактують по-різному, що зумовлено її циркулюванням у різних сферах життєдіяльності суспільства.

Аналіз розробок науковців свідчить, що категорія «інформація» має міжгалузевий характер, оскільки важлива для різних галузей як публічного, так і приватного права. Інформація, яка здійснює обіг у різних сферах діяльності суспільства, перетворюється на знання у тому випадку, якщо вона сприймається, селекціонується, аналізується і зберігається суб'єктом та може використовуватися ним цілеспрямовано та практично. Якщо інформація, отримана суб'єктом, не проходить шлях подібної обробки, то відповідно вона не може бути використана у діяльності і тому не перетворюється на знання. Іншими словами, будь-які знання являють собою інформацію, але не вся інформація може перетворитися на знання [140, с. 19 – 20].

Кормич Б.А. пропонує класифікувати властивості інформації за двома групами, а саме на загальні та юридичні. Загальні властивості – це ті, що характерні будь-якій інформації та використовують в суспільстві і мають вплив на всі суспільні відносини, незважаючи на наявність чи відсутність нормативно-правового регулювання. До таких властивостей належать: системність інформації, її селективність, невичерпність, субстаційна несамостійність інформації, здатність до поширення та трансформації. Юридичними властивостями інформації є ті, що безпосередньо зумовлюють особливості нормативно-правового регулювання суспільних відносин в інформаційному просторі, до яких належать: фізична невідчужуваність

інформації, необхідність її відособлення, незалежність прав на інформацію та її матеріальний носій, здатність до тиражування [93, с. 12].

Інші дослідники юридичними ознаками інформації визначають такі: можливість неодноразового використання необмеженим колом осіб та суб'єктів; здатність зберігати, накопичувати, інтегрувати; кількісна визначеність у встановлених організаційних формах; системність, універсальність, нематеріальність [60, с. 17].

У своїх дослідженнях Стаценко-Сургучова І.С. вказує, що система фіскальних органів спирається на інтелектуальну інформацію, до якої можна віднести економічну, правову, соціальну, статистичну та інші види інформації, а податкову інформацію дослідник розглядає як частину економічної. На думку науковця, економічна інформація є відображенням суспільно-економічних відносин і процесів за допомогою цифр, фактів, даних тощо. Вона є органічною частиною системи господарського механізму, оскільки забезпечує зв'язок між елементами і процесом відтворення. До основних джерел економічної інформації належать: бухгалтерський, статистичний й оперативний облік, розрахункова, планова і прогнозна документація, різноманітні публікації, матеріали телебачення, Інтернет тощо. Науковець зазначає, що всі ці характеристики стосуються й податкової інформації з тією тільки відмінністю, що податкова інформація – це відображення за допомогою цифр, фактів, даних та інших різноманітних матеріалів у сфері оподаткування [144, с. 16].

Під час реалізації завдань та функцій, покладених законодавством на органи ДФС України, ними передусім використовується податкова та митна інформації. Інші види інформації відіграють допоміжну роль, що зумовлюється специфікою діяльності органів ДФС.

Отже, оскільки тема нашого дослідження стосується питань інформаційних відносин у діяльності органів ДФС України, то вважаємо доцільним дослідити самі поняття податкової та митної інформації.

Розглянемо насамперед визначення податкової інформації, подані

науковцями.

Так, Дмитренко Е.С. розуміє податкову інформацію, як сукупність відомостей і даних щодо обчислення й сплати податків, зборів та обов'язкових платежів, створених, наданих, зібраних, одержаних, збережених, накопичених, оброблених, переданих, використаних, поширених, оприлюднених на матеріальних носіях або відображених в електронному вигляді, що підлягають аналізу, охороні та захисту [77, с. 42].

У свою чергу, Субіна Т.В. вважає, що податкова інформація – це та інформація, що стосується об'єкта та суб'єкта сфери оподаткування і використовується з метою адміністрування податків, зборів й інших обов'язкових платежів. Науковець зазначає, що використання інформації в органах ДФС України зумовило процеси розвитку інформатизації [147, с. 25]. На нашу думку, таке трактування є більш доцільним, адже воно відображає всі сторони інформаційної діяльності органів ДФС, встановленої законодавством.

Поняття «податкова інформація» у Податковому кодексі України (далі – ПК України) використовується у значенні, встановленому Законом України «Про інформацію» [22], та визначається як сукупність відомостей і даних, створених або отриманих суб'єктами інформаційних відносин у процесі поточної діяльності і необхідних для реалізації покладених на контролюючі органи завдань і функцій.

Основними документами, що відображають і підтверджують податкову інформацію, є: реєстри бухгалтерського обліку й облікові документи, адже всі фінансово-господарські операції платника податків, зборів та обов'язкових платежів пов'язані з визначенням об'єкта оподаткування і податкових зобов'язань, мають бути чітко зафіксовані у первинних документах. Податкова інформація може збиратися, зберігатися та опрацьовуватися в інформаційних системах ДФС України або безпосередньо службовими особами [127, с. 275].

До податкової інформації належать:

– відомості, що вносяться до звітних документів, пов’язані з обчисленням і сплатою загальнодержавних та місцевих податків і зборів;

– відомості, які подають до органів ДФС платники податків і зборів для взяття їх на податковий облік;

– відомості про облік доходів, витрат та інших показників, пов’язаних із визначенням об’єктів оподаткування (податкових зобов’язань), який ведеться платниками податків і зборів у встановленому порядку;

– відомості, відображені в документах, пов’язаних з обчисленням та сплатою податків та зборів;

– відомості про суми коштів, не сплачених до бюджету в зв’язку з отриманням податкових пільг і напрями їх використання;

– інформація, відображена в Державному реєстрі фізичних осіб – платників податків, Єдиному банку даних про платників податків – юридичних осіб, та інших реєстрах, ведення яких покладено законодавством на органи ДФС України;

– інформація щодо ліцензування діяльності суб’єктів господарювання з виробництва спирту, алкогольних напоїв і тютюнових виробів;

– відомості щодо розпорядження безхазяйним майном та іншим майном, що переходить у власність держави;

– відомості про фінансово-господарські операції платників податків;

– інформація, що надійшла від органів виконавчої влади, органів місцевого самоврядування та Національного банку України;

– відомості про встановлені ставки місцевих податків, зборів органами місцевого самоврядування та надані такими органами податкові пільги;

– інформація про дозволи, ліцензії, патенти, свідоцтва на право провадження окремих видів діяльності,

– відомості про експортні та імпортні операції платників податків;

– відомості, що надходять від банків, інших фінансових установ щодо наявності та рух коштів на рахунках платника податків;

– відомості від органів влади інших держав, міжнародних організацій або нерезидентів;

– інформація, отримана за результатами податкового контролю [5].

Щодо поняття митної інформації, то на сьогодні воно як на законодавчому рівні, так і у наукових роботах дослідників детально та ґрунтовно не вивчалося.

Дослідження порядку здійснення митної діяльності дозволило визначити, що митна інформація використовується у ході реалізації заходів митного контролю, митного оформлення, вона необхідна для митного забезпечення органів ДФС України.

Водночас потрібно зауважити, що поняття «митна інформація» ні в Митному кодексі України (далі – МК України), ні в Законі України «Про інформацію» не закріплено. Тому, для уникнення суперечностей щодо порядку використання та зберігання митної інформації органами ДФС, у тому числі під час її внесення до інформаційних систем та баз даних, вважаємо доцільно це поняття чітко закріпити у ст. 10 Закону України «Про інформацію» та окремо визначити у статті в такій редакції: «Митна інформація – це коло відомостей і даних, що збирається, використовується та накопичується органами ДФС для реалізації державної митної політики».

Документами, що відображають митну інформацію, є такі: декларація митної вартості та документи, що підтверджують значення складових митної вартості; зовнішньоекономічні договори, контракти або документи, які їх замінюють; рахунок-фактура або рахунок-проформа; банківські платіжні документи; транспортні документи; страхові документи та інші, передбачені Митним кодексом України [6].

До митної інформації належать:

– відомості, отримані за результатами митного контролю та оформлення про транспортні засоби комерційного призначення, що переміщуються через митний кордон України, товари, та які відображаються у митних деклараціях, документах, необхідних для здійснення митних процедур;

– відомості щодо справляння митних платежів платників;

– відомості, що стосуються ведення митної статистики про переміщення товарів через державний кордон України. У ч. 2 ст. 448 Митного кодесу України зазначено, що статистична інформація, яку формують і аналізують митні органи, використовується в інтересах зміцнення зовнішньоекономічних зв'язків, покращення митно-тарифного та нетарифного регулювання зовнішньоекономічної діяльності, подальшої інтеграції України у загальносвітову систему економічних відносин;

– відомості, що відображені в Українській класифікації товарів зовнішньоекономічної діяльності, до якої відноситься інформація про товари, і які при декларуванні підлягають класифікації;

– відомості, отримані в ході здійснення державного контролю нехарчової продукції при її ввезенні на державну територію України [6].

Використання податкової й митної інформації в органах ДФС за режимом доступу розподіляється на відкриту інформацію та інформацію з обмеженим доступом.

Відкритою є інформація, яка не віднесена законодавством до інформації з обмеженим доступом, за своєю суттю вона є публічною.

Чинним законодавством публічна інформація розглядається, як задокументована й відображена різноманітними засобами та на будь-яких носіях інформація, що отримана або створена в ході виконання суб'єктами владних повноважень своїх завдань та обов'язків, або така, що перебуває у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації [31].

Враховуючи специфіку функціональних обов'язків службових осіб органів ДФС, останні при використанні публічної інформації не отримуть якихось спеціальних дозволів чи погоджень. Отримання доступу до такої інформації здійснюється відповідно до процедури та порядку, зазначених у законах України «Про доступ до публічної інформації», «Про захист

персональних даних», а також інших законних та підзаконних нормативно-правових актів.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [22]. Далі розглянемо кожен вид окремо.

1. Згідно із Законом України «Про інформацію» конфіденційною визнається інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Така інформація може поширюватися лише за бажанням або згодою відповідної особи у передбаченому нею порядку згідно з визначеними нею умовами, й у інших випадках, визначених законодавством [22]. Аналогічне поняття конфіденційної інформації передбачено Законом України «Про доступ до публічної інформації» [31].

Науковці конфіденційність розглядають, як недоступність інформації для несанкціонованого доступу. Така властивість може забезпечуватися в органах ДФС як технічними способами захисту інформації, так і спеціальними режимними засобами та криптографічними методами [127, с. 277].

На нашу думку, інформація є конфіденційною під час її використання органами ДФС в тому випадку, коли вона отримується від фізичних та юридичних осіб і використовується для реалізації положень Податкового й Митного кодексів України. Така інформація зазвичай містить персональні дані, відомості щодо ведення фінансово-господарської діяльності, комерційну таємницю тощо. Розголошення цих даних може завдати значної шкоди її власникам та потребує надійного захисту з боку органів ДФС.

У статті 11 Митного кодексу України закріплені вимоги щодо додержання конфіденційності інформації. Зокрема, інформація, що стосується митної сфери держави, отримана підрозділами ДФС, може використовуватися такими органами тільки для реалізації митних цілей і розголошуватися лише за наявності дозволу суб'єкта, осіб чи органу, що

надав таку інформацію, передаватися третім особам, у тому числі іншим органам державної влади [6].

Відомості про фізичних та юридичних осіб, а також дані щодо товарів, транспортних засобів, які перетинають митний кордон України, що використовуються та формуються фіскальними органами, вносяться до інформаційних баз даних і можуть бути використані з дотриманням обмежень, встановлених для використання конфіденційної інформації. Несанкціоноване розголошення інформації органами ДФС призводить до настання юридичної відповідальності, передбаченої чинним законодавством.

2. Відповідно до Закону України «Про доступ до публічної інформації» таємною є інформація, доступ до якої обмежується та розголошення якої може завдати шкоди особі, суспільству і державі. Таємною є інформація, що містить державну, професійну, банківську таємницю, таємницю досудового розслідування й іншу передбачену законодавством таємницю [31].

В ДФС України інформація визнається таємною відповідно до Закону України «Про державну таємницю», в якому закріплено, що державна таємниця (секретна інформація) – це один з різновидів таємної інформації, що включає відомості таких сфер державної діяльності, а саме: оборони, економіки, науки, техніки, зовнішніх відносин, охорони правопорядку й державної безпеки та які визнані у встановленому законом порядку державною таємницею й підлягають державній охороні. Розголошення таких відомостей може завдати шкоди національній безпеці України [24].

Перелік інформації, яка віднесена до державної таємниці, закріплений у зводі відомостей, що становлять державну таємницю, та затверджений наказом Служби безпеки України № 440 від 12.08.2005 р. [48].

Посадові особи ДФС України підлягають притягненню до дисциплінарної, адміністративної та кримінальної відповідальності відповідно до чинного законодавства в разі порушення процедури порядку обігу та використання інформації, яка містить державну таємницу, якщо такі дії спричинили розголошення такої інформації.

3. Службовою визнається інформація: що відображається в документах суб'єктів органів державної влади, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони містять відомості щодо розробки напрямів діяльності установи або здійснення контрольних, наглядових функцій, процесів прийняття рішень і не обговорювались публічно; зібрана в ході оперативно-розшукової, контррозвідувальної діяльності, в оборонній сфері держави, яку не віднесено до державної таємниці. Документам, що містять службову інформацію, присвоюється гриф «Для службового користування» [24].

ДФС України 28 серпня 2014 року наказом № 88 затвердила перелік відомостей, які містять службову інформацію в органах ДФС України, до яких належить:

1) податкова інформація та перевірочна робота;

2) інформація з питань охорони державної таємниці, технічного та криптографічного захисту інформації;

3) відомості з питань інформатизації;

4) інформація щодо роботи з особовим складом;

5) інформація щодо правоохоронної діяльності;

6) інформація щодо мобілізаційної роботи та цивільного захисту;

7) не секретне діловодство, а саме відомості про втрату документів, виробів або інших матеріальних носіїв інформації, які містять службову інформацію і яким присвоюється гриф обмеження доступу «Для службового користування»;

8) митні питання [51].

Враховуючи певну ієрархію та формування системи інформації при застосуванні її в процесі обробки органами ДФС, в тому числі при прийнятті та реалізації управлінських рішень, таку інформацію умовно можна розподілити:

– за видом: податкова інформація; митна інформація; інші види інформації (правова, соціальна, економічна, науково-технічна тощо);

– за режимом доступу: відкрита (публічна) інформація – це загальнодоступна інформація, яка формується протягом діяльності, надається відповідними органами і розміщується в ЗМІ, офіційних документах; конфіденційна інформація; службова інформація; державна таємниця.

Як видно із зазначеного вище, органи ДФС працюють із великими потоками інформації. Тому вирішення завдання обробки значних обсягів інформації в процесі управління є найважливішим чинником удосконалення всієї системи управління в органах ДФС. Між інформаційною й організаційною структурами управління існує нерозривний зв'язок.

На сьогодні управління державою не може відбуватися без використання інформації. З огляду на це Афанасьєв В.Г. зазначає, що завдяки інформації здійснюється забезпечення прямого й зворотного зв'язку в системі управління [58, с. 19].

У свою чергу, Семир'янов Д.Я. зазначив, що інформація в управлінні виконує три рівні завдань:

1) є своєрідною формою зв'язку компонентів усієї системи управління з навколишніми зовнішнім світом;

2) інформація пов'язує всі функції управління, починаючи від підготовки й прийняття відповідного рішення до підведення підсумків щодо результатів його виконання;

3) є безпосередньою причиною, що визначає вибір системою іншого варіанту поведінки; переведення в новий стан такої системи, що забезпечує її рух до поставленої мети [139, с. 25].

Відповідно до зазначеного вище, можемо окреслити певні характеристики інформації, які є важливими складовими змісту адміністративно-правових відносин в органах ДФС:

1) своєчасне та якісне забезпечення службових осіб точною й достовірною інформацією;

2) можливість продуктивно та вчасно використовувати інформацію та посилатися на неї при безпосередньому здійсненні службових обов'язків

відповідними посадовими особами органів ДФС;

3) формування необхідного комфортного середовища, яке б давало змогу приймати якісні, продумані та зважені рішення на основі структурного глибокого аналізу отриманої інформації. Крім того, таке середовище повинно сприяти розвитку творчого потенціалу у співробітників ДФС;

4) якісне розуміння отриманої інформації, завдяки чому можна охарактеризувати отриману інформацію як за кількісними, так і за якісними показниками.

Отже для уникнення недоліків у законодавстві та формування консалідованого підходу щодо поняття митної інформації пропонуємо внести зміни до ст. 10 «Види інформації за змістом» Закону України «Про інформацію» та закріпити поняття митної інформації. Також вважаємо доцільно в окремій статті вказаного вище Закону викласти розуміння митної інформації.

## 1.2. Вплив державної політики на діяльність органів ДФС України у сфері забезпечення інформаційної безпеки

Національна безпека України має багато складових, у тому числі включає інформаційну безпеку. Інформаційна безпека передбачає дієвий комплекс заходів, що повинні надійно захищати фінансово-економічну, соціальну, політичну й інші сфери дільності держави, інтелектуальну власність осіб, а також відомості, що становлять передбачену законом таємницю. Отже, стабільний прогрес будь-якого суспільства в контексті розвитку демократичних, економічних, соціальних складових можливий лише за умови забезпечення інформаційної безпеки всіх без винятку суб’єктів інформаційних відносин, зокрема в податковій і митній сферах державної діяльності.

У зв'язку зі зростанням глобальних викликів та загроз забезпечення надійних та функціональних умов захисту й розвитку інформаційних процесів повинно бути надано державним структурам, оскільки тільки державний апарат, який сприається на високоорганізовані структури, здатний забезпечити належну інформаційну безпеку держави.

Забезпечення інформаційною безпекою зумовлено, по-перше, потребою гарантування національної безпеки держави; по-друге, існуванням загроз інформаційній сфері України, які можуть нанести значну шкоду загальнонаціональним інтересам; по-третє, можливістю уникнення впливу на свідомість та поведінку особистостей за допомогою інформації. Створення надійної системи протидії загрозам, захист інформаційного простору країни, інформаційної інфраструктури, інформаційних ресурсів держави є головним завданням інформаційної безпеки [145, с. 90].

Враховуючи підвищення значення інформації та інформаційних технологій в органах державної влади, в тому числі ДФС України, терміни «інформаційна безпека», «інформаційний суверенітет», «захист інформації» та інші міцно ввійшли у соціальний лексикон. Коли ведуть мову про інформаційні суспільства, то такі терміни є необхідними й обов'язковими його елементами. Коли ведуть мову про захист національного інформаційного простору, то мають на увазі насамперед державний інформаційний суверенітет, тобто належне володіння й розповсюдження всією спільнотою у державі відповідних національних інформаційних ресурсів [117, с. 103].

Інформаційний суверенітет – це виключне право держави вільно створювати та використовувати необхідні механізми та компоненти інформаційної інфраструктури відповідно до інформаційної політики країни за бюджетний кошт. При цьому в сучасному світі часто конфлікти супроводжуються застосуванням багатьох аспектів, у тому числі інформаційного.

Отже, формування інформаційної безпеки в Україні повинно супроводжуватися практичними заходами щодо реалізації відповідної державної політики у цій галузі шляхом:

а) гарантування, дотримання й забезпечення реальних прав і свобод кожного громадянина України, в тому числі в площині забезпечення права на вільне отримання і використання інформації;

б) формування відповідної інформаційної політики, яка б враховувала інтереси всіх верств населення та була доступною як на території України, так і поза її межами;

в) формування стратегії інформаційного захисту, відповідних служб та механізмів реалізації цієї політики через розвиток потужних інформаційних систем й елементів.

Науковці зазначають, що на сьогодні Україні необхідно зосередити увагу на таких ідеях: зробити внутрішній український інформаційний простір сучасним та конкурентоспроможним; забезпечити інформаційну присутність держави в світі та просувати позитивний імідж країни за кордоном, а також розробити механізми втілення цього в життя [128, с. 38]. Тому, для реалізації вказаного механізму держава розробляє політику щодо забезпечення інформаційної безпеки в органах влади.

Водночас зазначимо, що забезпечення інформаційної безпеки є важливим елементом державної політики щодо функціонування та розвитку податкової й митної систем. Така політика повинна забезпечувати відповідні гарантії безпеки інформаційних систем та механізмів, які використовують різні державні органи, зокрема ДФС, установи, приватні підприємства та організації.

Проаналізувавши стан сучасної системи інформаційної безпеки країни, можна виявити, що існують певні загрози у податковій й митній системах, пов’язані з їхнім функціонуванням.

Однією з суттєвих загроз інформаційній безпеці країни є можливість здійснювати атаки на інформаційне поле держави, руйнуючи та виводячи з

ладу інформаційні ресурси, здійснюючи вплив на суспільство, людей, з метою сформувати необхідну для агресора картину дійсності, підмінивши цінності, цілі, погляди та інтереси щодо важливих аспектів життєдіяльності у відповідному суспільстві. При цьому розвиток таких змін спрямований винятково на досягнення цілей ворожої сторони. Такі дії, які базуються на використанні інформаційних ресурсів, становлять собою загрозу державності та територіальній цілісності країни. Стратегічні дії є абсолютно новим механізмом впливу на свідомість населення цілої країни та можуть у сукупності з іншими методами та засобами або окремо призвести до вирішення поставлених ворожих завдань, навіть за відсутності застосування звичайних збройних сил та засобів.

Як зазначає Попова С.М., інформаційна безпека є обов'язковим елементом кожної зі сфер національної безпеки. Водночас, інформаційна безпека є самостійною сферою системи забезпечення національної безпеки держави. Належний рівень інформаційної безпеки України зумовлює її розвиток як суверенної, демократичної, правової та економічно стабільної держави [127, с. 273].

У свою чергу, дослідник Ліпкан В.А. визначає національну безпеку, як захист життєво важливих інтересів людини і громадянина, суспільства і держави, за якої здійснюється належний розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у всіх сферах життєдіяльності держави при виникненні певних негативних тенденцій [101, с. 233].

Основні напрями державної політики стосовно регулювання національної безпеки в інформаційній галузі визначено у статті 8 Закону України «Про основи національної безпеки України», а саме:

– забезпечення й гарантування інформаційного суверенітету нашої держави;

– обов'язкове дотримання основоположних прав людини та громадянина на свободу слова, безперешкодний доступ до відкритої інформації,

недопущення й перешкоджання діям органів державної влади та місцевого самоврядування щодо неправомірного втручання у діяльність засобів масової інформації;

– здійснення постійного вдосконалення державного управління й регулювання інформаційної галузі з урахуванням новітніх інформаційних тенденцій, впровадження інноваційних технологій, наповнення інформаційного простору, як внутрішнього так і світового, повною й достовірною інформацією про нашу державу;

– вжиття дієвих заходів щодо захисту інформаційного середовища України;

– запобігання, виявлення, протидія і боротьба з корупційними правопорушеннями, із зловживанням владою або службовим становищем, й іншими негативними факторами з використанням засобів масової інформації [33].

Головною інформаційною загрозою національній безпеці є загроза впливу протилежної сторони на розвиток інформаційних ресурсів країни, інформаційної інфраструктури, на сприйняття суспільства в цілому, здійснення впливу на прояви свідомості та підсвідомості особи, метою якого є нав’язування державі та громадянам своєї або вигідної системи цінностей, поглядів стосовно діяльності держави, для управління їхньою поведінкою та підштовхування протилежної сторони діяти у необхідному напрямі. Саме такі дії становлять загрозу суверенітету нашої держави в надзвичайно важливих сферах суспільства та держави, які реалізовуються шляхом інформаційної діяльності. Стратегічним інформаційним протистоянням на сьогодні називають абсолютно новий вид протистояння, що зможе врегулювати конфліктні ситуації між державами без притягнення до участі збройних сил країн.

Необхідно зазначити, що наукові дослідження, видання, навчальні посібники та засоби масової інформації України в процесі описання подій, явищ, процесів застосовують такі терміни: «інформаційна безпека», «безпека

інформаційної сфери», «безпека інформації». Це поняття близькі за значенням, але не ідентичні.

Змістом інформаційної безпеки є безпека інформаційної сфери та безпека інформації. Правова невизначеність інформаційної безпеки у загальному її розумінні викликає суперечності щодо виділення предметних ділянок і меж регулювання правовідносин, включаючи функції й повноваження суб'єктів у цій важливій сфері національної безпеки [116, с. 25].

Інформаційна безпека розуміється, як передбачений Конституцією України захист політичних, державних, громадських інтересів держави, загальнолюдських і національних цінностей.

Проаналізувавши Закон України «Про основи національної безпеки України», можна виявити, що він не містить чітко визначеного поняття інформаційної безпеки. Вона розглядається лише як одна із сфер національної безпеки, яку можна характеризувати певними специфічними загрозами національним інтересам [157, с. 26].

У Законі України «Про Основні засади розвитку інформаційного суспільства в Україні» визначено інформаційну безпеку, як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [10].

Водночас потрібно зауважити, що науковці донині не розробили єдиного підходу щодо визначення змісту поняття «інформаційна безпека». Деякі з учених зосереджують увагу на тому, що таке поняття здебільшого є станом. Інші вказують, що це процес. Окремі акцентують увагу на діяльності, системі гарантій, властивостях, функціях. Визначимо певні групи напрямів визначення цього поняття.

За визначенням Кормича В.А., інформаційна безпека відображає стан захисту гарантованих законом умов життєдіяльності держави, суспільства та окремої особи від внутрішніх та зовнішніх загроз [93, с. 14].

Під інформаційною безпекою також розуміють стан захисту людини, суспільства і держави, за якого охороняються інформаційні ресурси, здійснюється мінімізація шкоди від негативних інформаційних впливів, небажаних наслідків використання інформаційних продуктів та інформаційних технологій [141, с. 444].

Максименко Ю.Є. пропонує визначити інформаційну безпеку як результат управління реальними чи потенційними загрозами чи небезпеками з метою задоволення загальнонаціональних інтересів людини, суспільства та держави в інформаційній сфері [105, с. 16].

Линник Г.М. розуміє під інформаційною безпекою діяльність суб'єктів права, що передбачає задоволення національних інтересів у інформаційній сфері завдяки управлінню реальними чи потенційними загрозами [100, с. 9].

Більш змістовне визначення цього поняття подано у навчальному посібнику «Інформаційна безпека держави», в якому інформаційна безпека визначена як стан захищеності потреб людини, суспільства і держави в інформації, при якому їхнє існування і прогресивний розвиток забезпечується, незважаючи на наявність внутрішніх і зовнішніх інформаційних загроз [164, с. 38].

Даючи визначення інформаційної безпеки, Стоєцький О.В. виокремив кілька підходів щодо окреслення сутності цього поняття, зокрема здійснення заходів, спрямованих на захист: національних інтересів держави в інформаційному просторі; правил, передбачених законодавством, відповідно до яких здійснюються інформаційні функції в державі; інформаційного середовища, заходів керування небезпеками й загрозами, що, як наслідок, забезпечує державний інформаційний суверенітет; суспільних відносин, які передбачають життєво необхідні потреби особистості, громадянина, суспільства, країни в забезпеченні безпеки інформаційного простору. З

позиції адміністративно-правового підходу, цей науковець розглядає інформаційну безпеку як керування небезпеками та загрозами в інформаційному просторі, а також як процес, особливість, властивість, за допомогою чого забезпечується обрання оптимального шляху мінімізації негативних наслідків [146, с. 8].

Дослідник Зайцев М.М., у свою чергу, розглядає поняття «інформаційної безпеки», як стан захищеності важливих й основоположних цінностей та інтересів особистості, громадянина, суспільства та держави, за допомогою якої здійснюється стабільний розвиток й функціонування суспільства, забезпечується своєчасне виявлення, протидія й запобігання небезпекам, як реальним так і потенційним, що створюють загрозу державним інтересам у галузях інноваційної, наукової та технічної політики, загальнокультурного розвитку громадян, дотримання свободи слова, гарантування інформаційної безпеки, захисту інформації й інформаційних технологій у разі виникнення негативних тенденцій. Інформаційну безпеку він розглядає як складову частину національної [83, с. 234].

У процесі аналізу системи забезпечення інформаційної безпеки Ліпкан В.А. наголошує: «Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління» [101, с. 219-220].

У свою чергу, Петрик В.М. розуміє інформаційну безпеку як стан захищеності держави від спеціальних інформаційних операцій, актів зовнішньої інформаційної агресії, інформаційного тероризму, незаконного зняття інформації за допомогою спеціальних технічних засобів, комп’ютерних злочинів та іншого деструктивного інформаційного впливу, який завдає суттєвої шкоди національним інтересам [34, с. 122].

Інформаційну безпеку науковець Абакумов В.М. визначає як захист інформаційних відносин, пов’язаних із ними інформаційних процесів, за

якого досягається стабільний інформаційний розвиток, унеможливлюється інформаційний вплив, який має негативний характер, та негативні наслідки незаконного застосування інформаційних технологій в усіх сферах суспільного життя, унаслідок чого можна досягти створення та ефективного розвитку інформаційного суспільства в державі [53, с. 13].

Також інформаційну безпеку в енциклопедії для видавця та журналіста визначають, як захищеність державного інформаційного середовища, що формується, функціонує та розвивається з метою дотримання інтересів та цінностей громадян, суспільства і держави. Крім того, інформаційна безпека передбачає вжиття заходів щодо: захисту інформації від несанкціонованного зовнішнього або внутрішнього втручання; використання інформації чітко за цільовим призначенням для протидії негативному впливу на інформаційну чи другу сферу життєдіяльності як нашої держави, так і інших країн [67, с. 137].

В енциклопедичному словнику з державного управління поняття «інформаційна безпека» трактується, як система апаратних, програмних, організаційних та законодавчих заходів, спрямованих на забезпечення захищеності інформаційного простору держави від небажаного інформаційного впливу; національних інформаційних ресурсів, функціонування інформаційно-телекомунікаційних систем та інформації, яка циркулює в них [82, с. 294].

З погляду соціально-філософського осмислення інформаційну безпеку розуміють, як стан захищеності людини, суспільства та держави від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна існуванню, функціонуванню чи діяльності цих об’єктів у разі: а) використання неповної, несвоєчасної та невірогідної інформації; б) здійснення негативного інформаційного впливу; в) протиправного застосування інформаційних технологій; г) порушення цілісності, конфіденційності та доступності інформації [57, с. 10].

Найбільш поширене визначення поняття «інформаційна безпека» серед країн – членів Європейського Союзу таке: інформаційна (або мережева)

безпека – це захист інформації від несанкціонованого доступу; захист особистої інформації про відправників та одержувачів; створення надійного джерела постачання інформації, інформаційних послуг та необхідного обладнання; захист інформації, що безпосередньо стосується усіх аспектів національної безпеки (у тому числі військового потенціалу держави) [174].

У свою чергу, Березовська І.Р. розглядає інформаційну безпеку, як захист життєво важливих інтересів особи, суспільства і держави в інформаційній сфері від виникнення та впливу внутрішніх і зовнішніх загроз, що забезпечує її формування й стійкий розвиток в інтересах громадян, організацій, держави [64, с. 11]. Поділяємо думку науковця щодо доцільності виділити три сходинки адміністративно-правового процесу гарантування безпеки інформаційного простору: 1) інформаційний рівень свідомості самої особи (розвиток раціоналістичного та критичного напрямів мислення за допомогою використання основного принципу свободи вибору); 2) рівень суспільний, що досягається формуванням якісного інформаційного простору, плюралізму, багатоканальності в донесенні інформації до особи, справедливі та незалежні засоби масової інформації, що перебувають у власності вітчизняних підприємців; 3) найвища сходинка – державний рівень, який досягається інформаційним забезпеченням внутрішньої та зовнішньої політичної діяльності в міжнародній діяльності, організований захист інформації, що має перебувати в обмеженому доступі, запобігання правопорушенням у сфері інформаційної діяльності, комп'ютерним злочинам [64, с. 12].

У свою чергу, Субіна Т.В. визначила інформаційну безпеку на державному та міждержавному рівнях, як комплексну систему методів, заходів, засобів, спрямованих на дотримання інформаційного суверенітету держави, недопущення інформаційного впливу, що має негативний характер, на суспільство, окремих громадян, дотримання основоположних конституційних прав, свобод та законних інтересів людини і громадянина в інформаційній сфері, а також забезпечення належного рівня охорони і

захисту інформації та цілісності інформаційно-телекомунікаційних систем [147, с. 28].

На думку Мороза Д.О., під інформаційною безпекою потрібно розуміти захищеність інформації та інфраструктури, що її підтримує, від зовнішніх та внутрішніх дестабілізуючих впливів, що можуть нанести збитки власникам в особі органів ДФС України. Заходи стосовно забезпечення безпеки інформаційних систем, які використовують органи ДФС, умовно поділяють на такі види: 1) законодавчі, тобто ті, які відображено у нормах законів, підзаконних нормативних актах, відомчих наказах чи розпорядженнях чи певних міжнародних стандартах; 2) адміністративні, тобто дії, які можуть здійснюватися керівниками певних підрозділів через надані їм повноваження; 3) технічні, тобто заходи інформаційної безпеки, які регламентують певний порядок доступу та роботи з відповідною інформацією, інформаційними елементами та інформаційними ресурсами [62, с. 336].

На нашу думку, інформаційна безпека органів ДФС України становить певний стан захисту інформаційних баз даних, інформаційних систем, посадових осіб органів і служб ДФС, платників податків та зборів, при якому зводяться до мінімуму всі небажані наслідки використання інформаційних продуктів та інформаційних технологій. Належний та якісний захист інформації, яку використовують в органах ДФС України, є передумовою для забезпечення належної інформаційної безпеки.

Крім того, погоджуємось із Субіною Т.В., яка визначила правову категорію «адміністративно-правове забезпечення інформаційної безпеки в органах ДПС України», як сукупність правових норм, що регламентують суспільні відносини в інформаційній сфері і спрямовані на організаційне, правове та технічне забезпечення обігу інформації у фіскальних органах України [147, с. 35].

Підсумовуючи дослідження понятійного апарату, беручи до уваги думки науковців, вважаємо, що інформаційна безпека в діяльності органів

ДФС України – це стан захисту інформації, інформаційних технологій та інформаційних ресурсів, працівників служби, фізичних та юридичних осіб від неправомірних дій чи бездіяльності суб'єктів інформаційних відносин, за якого здійснюється виявлення, попередження та протидія інформаційним правопорушенням.

Аналіз перелічених підходів до трактування терміна «інформаційна безпека» дозволяє виокремити її такі сутнісні характеристики.

Інформаційна безпека органів ДФС України являє собою: по-перше, захищеність інформаційного середовища її підрозділів; по-друге, стан захищеності загальнонаціональних інтересів держави в інформаційному просторі, зокрема у сфері податкових і митних правовідносин; по-третє, захищеність встановлених законодавством правил та положень, згідно з якими здійснюються інформаційні процеси в ДФС України; по-четверте, суспільні відносини, які безпосередньо впливають на захист інтересів людини і громадянина, суспільства і держави у податковій й митній сферах від реальних й потенційних загроз, що можуть виникнути в інформаційному просторі; по-п'яте, обов'язкова складова економічної національної безпеки [101, с. 36].

Для адміністративно-правових засад забезпечення інформаційної безпеки в діяльності органів ДФС України використовують певні елементи цілісної структури, а саме: а) норми фінансового, інформаційного, адміністративного права, які закріплюють права та обов'язки учасників, які беруть участь у взаємовідносинах, пов'язаних з гарантуванням інформаційної безпеки в органах ДФС України; б) адміністративні та інформаційні правовідносини, які формуються протягом визначеної діяльності учасників взаємовідносин у податковій й митній сферах держави, мають безпосередній вплив на забезпечення інформаційної безпеки в органах ДФС України; в) законні й підзаконні нормативно-правові акти, які дозволяють реалізувати права та обов'язки взаємодіючих суб'єктів, що проявляється у втіленні

приписів норм адміністративного права протягом взаємовідносин суб'єктів забезпечення інформаційної безпеки в діяльності органів ДФС України.

Дослідники зазначають, що структурними елементами адміністративно-правових заходів і механізму адміністративно-правового регулювання є норми адміністративного права, адміністративно-правові відносини, акти тлумачення норм адміністративного права й акти реалізації адміністративно-правових норм [164, с. 49]. Деякі науковці пропонують таке визначення механізму адміністративно-правового забезпечення: «Це динамічна система правових форм, засобів і заходів впливу на поведінку суб'єктів через встановлення їхніх прав та обов'язків щодо створення, передачі, використання, зберігання, зміни, знищення конфіденційних службових відомостей, дія і взаємодія яких спрямовані на запобігання порушенню режиму службової таємниці чи на його відновлення у разі порушення» [164, с. 15].

На думку Степко О. М., головними складовими інформаційної безпеки ДФС України є: обсяг інформаційного продукту, що виробляється в державі і самою державою; здатність телекомунікаційних мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати процесом вироблення й поширення інформації; можливість доступу народу України до усіх інформаційних джерел, а також відкритість більшості з них [145, с. 90].

Інформаційна безпека ДФС України включає такі головні елементи: доступність, конфіденційність та цілісність. Доступність – це властивість інформації бути доступною й відкритою для користувача у зручний для нього час. Цілісність розуміється, як об'єктивність, точність, повнота й нерозривність інформації і програмного забезпечення. Конфіденційність, як властивість інформації, передбачає її захист від несанкціонованого доступу. [98, с. 167].

Так, у стандарті BS ISO/IEC 17799 Information security інформаційна безпека характеризується забезпеченням доступності, конфіденційності та

цілісності інформації, а в ISO/IEC 27001 – як «всі аспекти, пов'язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, невідмовності підзвітності, автентичності та достовірності інформації чи засобів її обробки». Ці визначення стосуються поняття «безпека інформації» і, до речі, більш-менш збігаються з вітчизняним нормативним визначенням, наведеним у «Концепції створення Єдиної державної автоматизованої паспортної системи», де безпека інформації розуміється як «захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводить до модифікації, розкриття чи руйнування даних». Хоча, на думку науковців, таке трактування безпеки інформації є дещо звуженим, оскільки не включає забезпечення доступності інформації. Українські стандарти з інформаційної безпеки певною мірою гармонізовані до закордонних стандартів типу ISO, в яких поняття «information security» перекладається як «безпека інформації» [74, с. 37].

Інформаційну безпеку ДФС України розглядають як єдину цілісність таких складових: персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому під час визначення характеру ризиків потрібно брати до уваги такі елементи:

– концептуальні засади політичної безпеки, її принципів, стандартів та правил, погоджених із діючим законодавством і принципами забезпечення безперервності інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;

– виділення об'єктів та цілей;

– визначення прийнятних з погляду гарантування прав та інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки та оцінки ризиків, управління ризиками;

– визначення статусно-функціональних ролей, очікувань та міри відповідальності задіяних суб'єктів включно зі звітністю про події, які несуть потенційні загрози [102, с. 89 – 90].

У забезпеченні інформаційної безпеки ДФС України важливе місце відведено Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації. Структуру Департаменту утворюють такі відділи: режимно-секретний відділ; відділ спеціального зв'язку та криптографічного захисту інформації; відділ забезпечення технічного захисту інформації та контролю; відділ захисту інформації в інформаційно-телекомунікаційних системах та контролю. Основним завданням Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації є організація, контроль та здійснення цілеспрямованих дій щодо охорони державної таємниці, технічного та криптографічного захисту інформації в органах ДФС України та його територіальних підрозділах. Крім того, він реалізує функцію із забезпечення в межах своїх повноважень положень державної політики щодо державної таємниці, захисту інформації, контроль за її збереженням в органах ДФС України [37].

Доцільно зауважити, що, фактично, більшість функціональних підрозділів ДФС України тією чи іншою мірою виконують завдання із забезпечення внутрішньої інформаційної безпеки.

Для того щоб виокремити перспективи інформаційного розвитку діяльності ДФС та сприяти зростанню рівня її загальної інформатизації, необхідно приділяти значно більше уваги цій проблемі в сучасних наукових дослідженнях. При цьому насамперед треба приділити увагу проблемі конфіденційності податкової та митної інформації, розробити дієві способи захисту від можливих інформаційних атак, щоб зберегти інформацію, що становить державну таємницю та зберігається в органах ДФС.

На нашу думку, безпека інформаційних систем та баз даних безпосередньо пов'язана зі станом захисту відповідної інформації органів ДФС, які здійснюють збір, обробку та використання такої інформації. Вказані дії органів ДФС можливі лише при виконанні останніми функцій щодо формування та впровадження контролю за фізичними і юридичними особами при здійсненні політики додержання податкового й митного

законодавства. При цьому, значна увага приділяється охороні інформаційних систем та баз даних і зменшенню ризиків несанкціонованого втручання в роботу таких систем, позаслужбового використання відповідної інформації. Ефективний захист інформаційних систем і баз даних є запорукою сталого розвитку країни та забезпечення безпосередньої інформаційної безпеки органів ДФС України.

У зв'язку з цим пропонуємо відокремлювати поняття «безпека інформації» та «інформаційна безпека». Інформаційну безпеку потрібно розглядати як заходи щодо створення, підтримання й захисту на належному законодавчому та технічному рівнях інформаційних систем органів ДФС України, основних прав і свобод людини. Безпеку інформації – як стан інформації, інформаційних ресурсів та інформаційних і телекомунікаційних систем, за якого з необхідною вірогідністю забезпечується її захист.

На думку науковців, безпека інформації – це захищеність інформації, що обробляється засобами обчислювальної техніки або автоматизованої системи від внутрішніх та зовнішніх загроз, від доступу осіб, які не мають такого права, її отримання, розкриття, модифікації або руйнування [57, с. 11].

З огляду на це, Гребенюк О.В. визначив безпеку інформації, як стан захисту інформації від навмисних або помилкових дій штучного або природного походження, що можуть нанести неприйнятний збиток учасникам інформаційних правовідносин, зокрема власникам інформації та її користувачам [75, с. 69].

Інформаційний простір, інформаційна інфраструктура та продукти інформаційної діяльності мають значний вплив на рівень соціально-економічного розвитку. Тому закономірністю є те, що під час використання інформаційних технологій в органах ДФС України у всіх напрямах діяльності підпищується кількість пов'язаних з такими інформаційними продуктами правопорушень, виникають передумови незаконного витоку податкової, митної та криміналістично значущої інформації. Це вимагає

застосування нових підходів у забезпеченні інформаційної безпеки органів ДФС України [131, с. 164].

Здійснюючи заходи щодо гарантування інформаційної безпеки в органах ДФС України, особливу увагу потрібно приділяти загрозам, які з'являються під час виконання функціональних обов'язків співробітниками ДФС України.

Науковці зазначають, що загрози інформаційній безпеці України загалом та безпеці зокрема у податковій й митній сферах – це сукупність чинників, що можуть становити небезпеку загальнодержавним інтересам, а також невід'ємним правам особи, внаслідок здійснення негативного інформаційного впливу на систему цінностей громадян, інформаційно-технічну інфраструктуру та інформаційні ресурси [112, с. 326].

Також, нами визначено загрози, що стосуються інформаційної безпеки у сфері митного контролю, як сукупність умов та суперечностей, які виникають у суспільстві, політичних, економічних, соціальних відносинах та які є причиною появи порушень у процесі реалізації державної митної політики, порушення якісних та цілісних характеристик інформації, а також внесення помилкової або невідповідної інформації до інформаційних, телекомунікаційних та інформаційно-телекомунікаційних баз даних, систем та засобів.

Науковці виокремлюють такі групи групи інформаційно-технічних небезпек:

– нові соціальні злочини, спрямовані проти особистості, суспільства, держави, з використанням сучасних інформаційних технологій (кібертероризм, кіберзлочинність, наприклад махінації з електронними грошима, комп'ютерне хуліганство та інші);

– використання сучасних інформаційних продуктів, інформаційних технологій у політичних цілях;

– контроль за життям, цілями громадян, політичних організацій за допомогою інформаційних мереж;

– активний розвиток інформаційної зброї, що може здійснювати вплив на психіку й свідомість людей, на технічну інфраструктуру суспільства [128, с. 38].

У Законі України «Про основи національної безпеки» визначено, що однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації». Іншими загрозами є: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [33].

Осередками потенційних загроз, які виникають через несанкціонований вхід до інформаційних систем та баз даних з використанням відповідних комп'ютерних програм та засобів, є суб'єкти, які своїми діями порушують порядок доступу до таких систем та баз даних. Цими суб'єктами, зазвичай, виступають: порушник, носій програми, апаратна закладка.

Самі загрози можна класифікувати так: відповідно до джерела походження; відповідно до середовища, на яке вони поширюються; за способом реалізації; відповідно до об'єкта та характеру впливу на інформацію; відповідно до уразливості, яка теоретично існує вже при розробці програми або бази даних.

При аналізі загроз, що виникають в інформаційному середовищі, потрібно враховувати: джерело, яке здійснює внутрішній або зовнішній вплив; мотивацію суб'єкта (наприклад, матеріальна вигода чи господарча перевага); періодичність виникнення (разове або постійне несанкціоноване отримання інформації) та їхня кількість.

Щоб забезпечити належну захищеність інформації та інформаційних систем в органах ДФС, необхідно використовувати відповідні моделі та

методи оцінки загроз і небезпек. Вони змінюються дуже часто з урахуванням розвитку новітніх технологій і залежать як від рівня розвитку конкретного суспільства, так і від контексту оцінки, наявності необхідних даних щодо характеристик загрози, алгоритму отримання даних щодо ймовірності настання та розміру негативних наслідків. Наявність відповідних відомостей із цього питання дозволяє досить точно визначити характер впливу інформації, яка використовується як посягання та рівень загрози і небезпеки.

Для оцінювання характеру негативного впливу небезпеки використовують різні дослідження загроз, що включають моделі, схеми, структури тощо. Такі дослідження можуть бути конкретними, концептуальними або статичними. Вони характеризують структуру, зв'язки і стани небезпек, а також загроз через прості або складні динамічні кількісні зміни в їхньому розвитку.

Усі загрози можна характеризувати за напрямом впливу так: ідентифікація потенційних небезпек; ідентифікація відмов; кількісна оцінка відповідних ризиків; визначення чинників, які сприяють виникненню ризиків та ненадійних ланок у системі; поглиблене розуміння функціонування системи; зіставлення ризиків системи, яка досліджується, з ризиками альтернативних систем; ідентифікація та порівняння ризиків і невизначеностей; можливість вибору засобів і способів зниження ризиків.

Одним з головних завдань моделювання загроз є обґрунтування рішень, пов'язаних із виникненням ризиків. До вихідних даних, потрібних для моделювання, можна віднести: перелік джерел загроз; перелік вразливостей; перелік загроз, пов'язаних із забезпеченням безпеки інформації; перелік руйнуючих дій, що виникають унаслідок реалізації негативних дій загроз; визначення коефіцієнтів виконання руйнуючих дій; визначення вірогідності наявності сприятливих умов, необхідних для використання вразливості для забезпечення безпеки інформації; наявність взаємозв'язків між джерелами, загрозами і вразливими елементами; наявність взаємозв'язків між загрозами і руйнуючими діями.

Відповідно, враховуючи позиції щодо негативних впливів на інформаційну безпеку, можна виділити такі основні небезпеки:

1) контролювання інформаційних ресурсів держави. Така небезпека може бути реалізована методами: протиправного проникнення в інформаційні системи, зокрема органів ДФС; законним шляхом при активній участі закордонних організацій протягом створення інформаційного каркасу держави. При цьому, крім негативних наслідків, пов'язаних з тим, що інформаційні ресурси країни схильні до контролю конкретних іноземних організацій, завдається пряма шкода економіці держави через те, що в такому випадку вітчизняна наука і виробництво залишаються без відповідних замовлень;

2) загроза знищення та дезорганізації інформаційних систем, що контролюються відповідними державними органами. Враховуючи сучасний стан розвитку інформаційних технологій, відповідні дії можуть виконуватися навіть у мирний час. Вони можуть нести загрозу через знищення важливих державних інформаційних систем, через спотворення або застосування негативної інформації, яка ставить за мету дезорганізувати або вплинути на прийняття неправильних рішень на відповідному рівні державного управління.

Для профілактики та боротьби з порушеннями в сфері сплати та адміністрування податків, зборів інформаційна безпека може розглядатись як необхідний елемент. Так, під час виконання органами ДФС України відповідних завдань їм стає відома інформація про платника податків, зборів, несанкціоноване використання якої може завдати шкоди господарським та діловим інтересам такого платника. Для запобігання цих негативних наслідків необхідно дотримуватися державної таємниці. Але чинним законом не визначено, як потрібно забезпечувати непоширення комерційної та особистої інформації про платника податків, зборів, відсутні конкретні приписи та положення щодо відповідальності посадових осіб органів ДФС за неправомірне поширення такої інформації.

Водночас органи Державної фіскальної служби України виконують ряд заходів щодо забезпечення інформаційної безпеки, які визначаються як комплекс організаційно-правових, технологічних, психологічних заходів, і спрямовані на попередження, усунення порушень і загроз податковій, митній інформації, схоронності конфіденційних даних платників податків, зборів, що можуть завдати шкоди фізичним чи юридичним особам, органам ДФС України і державі в цілому.

Отже, головним завданням органів ДФС України щодо забезпечення інформаційної безпеки є дотримання безпеки комбінацій доступу до інформаційних систем та баз даних, цілісності та конфіденційності інформації, яка в них міститься. Такі принципи передбачають можливість своєчасно отримувати, обробляти та зберігати необхідну інформацію, а також запобігати невідповідній відмові в отриманні такої інформації; приймати рішення у випадках незаконної трансформації або знищення інформації; запобігати несанкціонованому поширенню інформації.

Крім того, державна політика впливає на інформаційну безпеку в Україні, зокрема органів ДФС, унаслідок забезпечення дотримання основних прав, свобод людини і громадянина, включаючи його права на володіння і користування інформацією; гарантування максимально доступної інформаційної політики для всіх користувачів за межами України; захищеності національного інформаційного середовища та потужного розвитку новітніх інформаційних технологій в органах ДФС.

## 1.3. Суб’єкти, що забезпечують інформаційну безпеку в органах ДФС України

Конституцією України чітко визначено, що захист суверенітету та територіальної цілісності України, здійснення заходів, спрямованих на гарантування її економічної та інформаційної безпеки, є найважливішими

функціями держави та справою всього Українського народу. Доцільно зауважити, що основними складовими інформаційної безпеки є такі елементи: суб'єкти, які беруть участь у правовідносинах при здійсненні інформаційних процесів, пов'язаних з отриманням, обробкою, використанням, розпорядженням інформацією тощо; об'єкти – те, заради чого та у зв'язку з чим суб'єкти вступають в інформаційні правовідносини; поведінка (дії, бездіяльність) суб'єктів, яка виникає під час здійснення інформаційних правовідносин.

Так, об'єктами інформаційних правовідносин можуть виступати: інформаційні продукти, послуги та документована інформація; виключні права; складові елементи інформаційної безпеки (інформаційні права і свободи особи, стан захищеності особистості, захищеність інформації, інформаційних ресурсів, тощо); інформаційні технології та засоби їхнього забезпечення, інші об'єкти в інформаційній сфері; взаємні права, обов'язки і відповідальність суб'єктів правовідносин при реалізації інформаційних процесів. Також науковці виокремлюють такі групи суб'єктів інформаційних відносин: виробники інформації, її автори; власники інформації або інформаційних об'єктів; споживачі інформації [60, с. 5].

Законодавець у ст. 4 Закону України «Про інформацію» суб'єктами інформаційних відносин визнає фізичних та юридичних осіб, об'єднання громадян, суб'єктів владних повноважень. Об'єктом інформаційних відносин виступає інформація [22].

У своєму дисертаційному дослідженні Шпенов Д.Ю. зазначає, що суб'єкти інформаційного права є сторонами інформаційних правовідносин та носіями взаємних прав і обов'язків, закріплених інформаційно-правовими нормами. Суб'єкти інформаційних правовідносин за кількісною ознакою можуть бути індивідуальними або колективними. Фізичні особи визнаються індивідуальними суб'єктами, а саме: громадяни України, іноземні громадяни, особи без громадянства. Відповідно, колективними суб'єктами інформаційних відносин є юридичні особи, а саме: органи державної влади,

органи місцевого самоврядування, об’єднання громадян, засоби масової інформації, провайдери інформаційних автоматизованих мереж, суб’єкти господарювання, що займаються електронною комерцією, статистичні установи, архівні установи, бібліотеки й інші структури різноманітних форм власності [163, с. 13].

Об’єкт правовідносин містить у собі певну множинність об’єктів: 1) інформацію; 2) матеріальний достаток, розгалуженість інформаційних систем, інформаційних ресурсів, наявність баз даних, засоби, що гарантують автоматизованість інформаційних технологій, обчислювальну техніку та зв’язок; 3) сукупність нематеріальних особистих благ (забезпечення таємниці особистого життя, сімейні таємниці, захист честі, ділової репутації); 4) характеристика поведінки та дій учасників інформаційних правовідносин. Такі правові відносини характеризуються як матеріальним, так і юридичним змістом. Матеріальний об’єкт зосереджує в собі фактичні інформаційні правовідносини, що гарантуються в нормах інформаційного права; юридичний зміст означає сукупність прав та обов’язків сторін інформаційних правовідносин. Передумовами виникнення згаданих вище правовідносин є формально-юридичні обставини, що містять в основі норму права, правоздатність та дієздатність учасників правовідносин та базуються на юридичному факті.

Інформаційні відносини виникають, розвиваються і припиняються в суспільстві при самостійному циркулюванні інформації, при створенні та використанні новітніх інформаційних технологій, систем і механізмів інформаційної безпеки [163, с. 14].

Шевчук О.М. виокремлює особливі інформаційні відносини, безпосереднім об’єктом яких є інформація в електронно-цифровій формі. Головним предметом нормативно-правового регулювання таких відносин виступають соціальні відносини, що виникають і розвиваються у процесі створення та використання інформації внаслідок застосування автоматизованих інформаційних систем. Такі відносини називають

інформаційно-комп'ютерними, вони є різновидом інформаційних відносин. Діяльність учасників інформаційно-комп'ютерних відносин відносять до галузі комп'ютерної інформації. Специфіка зазначених відносин зумовлена особливостями самої природи інформації на машинних носіях і безпосередньої технології її обробки. Запровадження інформаційних систем та технологій супроводжують суспільні відносини, що виникають при: гарантуванні й забезпеченні конституційних прав людини і громадянина на інформацію за допомогою інформаційних технологій; розробці, створенні, впровадженні та експлуатації комп'ютерних мереж та систем, а також телекомунікаційних мереж; створенні, поширенні, передачі, купівлі-продажу програмного забезпечення для електронно-обчислювальних машин та інших автоматизованих інформаційних систем; формуванні й опрацюванні інформаційних ресурсів, що включають електронні бази даних; установленні й дотриманні режиму доступу до інформації в інформаційних системах і проведенні інших заходів інформаційної безпеки; міжнародному обміні комп'ютерною інформацією [161, с. 15].

Враховуючи різні підходи науковців, вважаємо, що суб'єкти, які є учасниками інформаційних відносин в органах ДФС, виконують обов'язок забезпечення інформаційної безпеки об'єктів таких відносин з урахуванням законодавчо закріплених вимог. Об'єктами інформаційної безпеки в органах ДФС виступають інформація, інформаційні ресурси, бази даних, інформаційно-телекомунікаційні системи, програмні забезпечення, технології тощо.

Розглянемо суб'єктів забезпечення інформаційної безпеки в органах ДФС України та їх повноваження, передбачені законодавством України.

Так, Основним Законом України в ч. 3 ст. 17 закріплено перелік суб'єктів, на які покладаються обов'язки щодо забезпечення й гарантування державної безпеки, а також виконання комплексу інших дій, спрямованих на забезпечення національної безпеки України відповідними військовими формуваннями та правоохоронними органами держави [1].

Не зважаючи на те що Конституцією України захист суверенітету, територіальної цілісності, економічної та інформаційної безпеки визнано найважливішими функціями держави, в ній не вказано, які саме органи державної влади їх здійснюють.

Проаналізувавши норми Конституції України, а також положення Закону України «Про основи національної безпеки України», можна визначити суб'єктів забезпечення й гарантування інформаційної безпеки в органах ДФС України, якими є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; Національний банк України; міністерства й інші центральні органи виконавчої влади; суди; прокуратура України; місцеві державні адміністрації й органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; правоохоронні органи; громадяни України, об'єднання громадян.

Так, враховуючи положення Конституції України та Закону «Про основи національної безпеки» [33], доцільно виокремити такі повноваження згаданих вище суб'єктів забезпечення й гарантування інформаційної безпеки в органах ДФС України:

1) Президент України, як голова держави, організовує загальнодержавне керівництво у всіх сферах національної безпеки України та в такому напрямі діяльності опирається на Раду національної безпеки та оборони.

У січні 2002 року Указом Президента України при Раді національної безпеки та оборони створено Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки, яка теоретично є консультативно-дорадчим органом. Основними функціями цієї Комісії є:

– аналіз стану національної безпеки України, виявлення можливих загроз в інформаційній сфері, опрацювання та узагальнення міжнародного досвіду щодо реалізації й формування інформаційної політики в державі;

– аналіз виконання галузевих програм та заходів державної політики в інформаційній сфері, які реалізуются міністерствами й іншими центральними органами виконавчої влади;

– розроблення і внесення пропозицій Президентові України та РНБО щодо виділення національних інтересів держави в інформаційній сфері, основоположних підходів до формування й дієвого функціонування державної інформаційної політики та гарантування інформаційної безпеки України;

– виконання заходів щодо вдосконалення інформаційної політики України, реалізація державної стратегії розвитку і захисту національного інформаційного простору, входження України у світовий інформаційний простір;

– удосконалення системи нормативно-правового та наукового забезпечення інформаційної безпеки України;

– забезпечення розвитку інформаційної інфраструктури держави;

– організація міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;

– удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України у сфері національної безпеки й оборони [43].

Ця Комісія має дорадчо-консультативний статус, однак її рішення мають розглядатись органами місцевого самоврядування, органами виконавчої влади, підприємствами, установами та організаціями. До складу Комісії за посадою входять керівники чи заступники міністерств, відомств, правоохоронних органів (у тому числі СБУ), представники Генерального штабу ЗС України, державних комітетів, комітетів Верховної Ради України, наукових та дослідницьких установ, діяльність яких стосується проблематики інформаційної безпеки. Такий представницький склад створює теоретичні можливості для всебічного та об’єктивного реагування на

небезпеки й загрози, що можуть виникнути в інформаційній сфері, надає можливість ефективної міжвідомчої співпраці [43].

Необхідно зауважити, що в складі Комісії не передбачено створення окремого відділу, що мав би займатися моніторингом просторів інформації та надавав оперативну й достовірну інформацію щодо перспективи наявних загроз інформаційній безпеці держави та органам виконавчої влади.

2) Верховна Рада України, діючи в конституційних межах, встановлює основні принципи внутрішньої та зовнішньої політики держави, визначає основоположні засади у сфері національної безпеки, відповідно забезпечує формування законодавчої бази щодо гарантування інформаційної безпеки.

Український парламент має в своєму складі комітет Верховної Ради, що займається питаннями інформаційної безпеки та свободи слова. Основний напрям діяльності створеного органу – розробка та впровадження інновацій у законодавчу базу країни з метою регулювання інформаційних відносин, діяльності засобів масової інформації та сприяння утвердженню свободи слова.

Предметом відання цього комітету є:

– національна політика в інформаційній сфері та інформаційній безпеці;

– забезпечення основоположних прав громадян на інформацію;

– гарантування свободи слова;

– регулювання діяльності друкованих та електронних засобів масової інформації, Інтернету;

– інформування про діяльність Верховної Ради України;

– принципи реалізації рекламної діяльності [34].

Комітет проводить підготовку та розробку нормативних актів, які стосуються та регулюють функціонування електронних та друкованих засобів масової інформації, рекламних правовідносин, розвиток Інтернету. Здійснюючи діяльність, комітет використовує інформацію Державного комітету України з питань інформаційної політики, телебачення і радіомовлення, Національної ради України з питань телебачення і

радіомовлення, Державного комітету зв'язку та інформатизації України і тісно співпрацює з ними.

Здійснюючи підготовку законопроектів, комітет залучає провідних вітчизняних фахівців у сфері інформаційного законодавства, співпрацює з Громадською радою з питань свободи слова та інформації. Крім того, комітет ініціює й організовує слухання у Верховній Раді України щодо питань інформаційних відносин в Україні, розглядає звернення громадян у випадку порушен їх прав і свобод на інформацію [43].

3) Кабінет Міністрів України – вищий орган виконавчої влади, який організовує забезпечення економічної самостійності держави, суверенітету України, вживає дієвих заходів для дотримання прав і свобод людини і громадянина, національної безпеки, правопорядку.

Законом України «Про телекомунікації» у ст. 14 перелічено функції Кабінету Міністрів України в інформаційній сфері, а саме:

– дотримання рівних умов розвитку всіх форм власності у сфері телекомунікацій;

– реалізація національної політики щодо телекомунікацій;

– забезпечення управління об'єктами державної власності у сфері телекомунікацій;

– координація діяльності міністерств, інших центральних органів виконавчої влади у сфері телекомунікацій [28].

У сфері користування радіочастотним ресурсом України Кабінет Міністрів, керуючись ст. 10 Закону України «Про радіочастотний ресурс», реалізує такі функції:

– затверджує Національну таблицю розподілу смуг радіочастот і План використання радіочастотного ресурсу України;

– координує діяльність центральних органів виконавчої влади щодо управління і користування радіочастотним ресурсом України;

– забезпечує здійснення конверсії радіочастотного ресурсу України в обсягах та в терміни, передбачені Планом використання радіочастотного ресурсу України;

– встановлює розмір зборів за користування радіочастотним ресурсом України;

– встановлює розмір плати за видачу, переоформлення, продовження терміну, видачу дубліката ліцензій на користування радіочастотним ресурсом України [26].

Кабінет Міністрів України здійснює вказані повноваження за допомогою Національної комісії, яка забезпечує державний контроль і регулювання у сфері зв'язку та інформатизації. Національна комісія є органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом й надання послуг поштового зв'язку. У визначеній сфері Національна комісія здійснює повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю) [44].

Також повноваження щодо забезпечення інформаційної безпеки та захисту інформаційного середовища здійснює Державний комітет України з телебачення і радіомовлення. Він є основним органом у системі центральних органів виконавчої влади, який здійснює формування й реалізацію національної політики у галузі телебачення та радіомовлення, видавничій й інформаційній сфері [36]. Крім того, Національна рада України з питань телебачення і радіомовлення – це конституційний, колегіальний орган виконавчої влади, який здійснює нагляд за дотриманням законів держави у галузі телерадіомовлення та виконує регуляторні повноваження щодо аудіовізуальних ЗМІ [15].

Необхідно зазначити, що Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сферах національної безпеки; виокремлює стратегічні національні інтереси держави,

концептуальні підходи до забезпечення національної безпеки у інформаційній та інших сферах державної діяльності [16].

5) Національний банк України згідно з діючим законодавством визначає, формує і реалізує грошово-кредитну політику для забезпечення національної безпеки держави.

6) Міністерства, інші центральні органи виконавчої влади, Служба зовнішньої розвідки України, Служба безпеки України в межах наданих законодавством їм функцій і повноважень здійснюють реалізацію передбачених Конституцією, законами України, актами Президента України, Кабінету Міністрів України завдань, забезпечують виконання концепцій та програм в інформаційній сфері.

Державна служба спеціального зв'язку та захисту інформації України є головним органом, що забезпечує інформаційну безпеку. Основні завдання цього органу такі: організація функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку й інших завдань, передбачених законодавством [17].

7) Місцеві державні адміністрації, органи місцевого самоврядування здійснюють практичне вирішення завдань у галузі національної безпеки, у тому числі в інформаційній сфері, віднесених діючим законодавством до їхніх повноважень.

8) Органи цивільного захисту забезпечують захист населення, території України від надзвичайних ситуацій як у мирний час, так і в особливий період.

9) Правоохоронні органи здійснюють виявлення, протидію, боротьбу із злочинністю, а також профілактику правопорушень у сфері забезпечення інформаційної безпеки, зокрема в органах ДФС.

10) Суди загальної юрисдикції здійснюють судочинство, зокрема у справах про злочини, що завдають шкоди національним інтересам держави в інформаційній сфері.

12) Прокуратура України виконує свої повноваження згідно із Конституцією України та Законом України «Про прокуратуру України».

13) Наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, у сфері інформаційної безпеки, зокрема Національний Інститут проблем міжнародної безпеки. Відповідно до пункту 9 Статуту, затвердженого Указом Президента України від 29 липня 1997 р. № 719, цей Інститут здійснює дослідження стану інформаційної безпеки України, її присутності у світовому просторі; сприяє позитивному іміджу держави, політичним та економічним проектам, які запроваджуються [41].

14) Громадяни України реалізують й забезпечують національні інтереси опосередковано, беручи участь у виборах, референдумах, через органи державної влади та місцевого самоврядування. Громадяни, добровільно виконуючи свої конституційні обов'язки перед державою, реалізують заходи, передбачені законами України, для забезпечення національної безпеки, в тому числі в інформаційній сфері. Безпосередньо або через об'єднання громадян вони привертають увагу суспільних й державних інститутів до загроз і небезпечних процесів у різноманітних галузях життєдіяльності держави, використовуючи законодавчі приписи, самостійно захищають свої права та інтереси, особисту безпеку.

Однак комплексні завдання й повноваження суб'єктів у сфері забезпечення інформаційної безпеки органів ДФС діючим законодавством країни не передбачені.

Наприклад, у ст. 4 Закону України «Про основи національної безпеки України» закріплено перелік суб'єктів, які забезпечують національну безпеку, а в ст. 9 визначено їх повноваження. Водночас, адміністративно-

правові відносини й повноваження суб'єктів забезпечення інформаційної безпеки регулюються законодавчими актами тільки у сфері захисту державної таємниці, технічного захисту інформації та декларуються на деяких інших напрямах забезпечення інформаційної безпеки [33].

У ст. 4 Закону України «Про державну таємницю» визначено, що державна політика стосовно державної таємниці є однією із складових внутрішньої та зовнішньої політики, яку визначає Верховна Рада України. У ст. 5 цього Закону закріплено повноваження органів державної влади, місцевого самоврядування, їх службових осіб у галузі охорони державної таємниці, а саме:

– Президент України, здійснюючи заходи із забезпечення національної безпеки, видає розпорядження й укази, які стосуються охорони державної таємниці;

– Рада національної безпеки і оборони України здійснює координацію і контроль за діяльністю державних органів у галузі забезпечення охорони державної таємниці;

– Кабінет Міністрів України спрямовує діяльність міністерств, інших органів виконавчої влади з метою організації виконання державної політики з охорони державної таємниці;

– центральні та місцеві органи виконавчої влади, місцевого самоврядування реалізують державну політику з охорони державної таємниці в межах наданих законодавством повноважень;

– Служба безпеки України є спеціально уповноваженим державним органом, який здійснює контроль щодо забезпечення охорони державної таємниці.

Крім того, дотримання охорони державної таємниці з обов'язковим урахуванням вимог режиму секретності в органах державної влади, місцевого самоврядування, на підприємствах, установах та організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників таких органів, підприємств, установ і організацій [24].

Служба безпеки України здійснює контроль за додержанням законодавства про державну таємницю згідно з положеннями Закону України «Про Службу безпеки України». Цей орган державної влади має повноваження контролювати стан охорони державної таємниці в усіх державних органах, місцевого самоврядування, на підприємствах, в установах і організаціях. Також, під час реалізації цих завдань Служба безпеки України може одержувати безоплатно інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, складені за результатами контролю стану охорони державної таємниці та викладені в актах офіційних перевірок, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їхніх форм власності [21].

Відповідно до структури організаційно-штатного розпису, який діє на сьогодні, суб'єктами забезпечення інформаційної безпеки в органах ДФС України є такі підрозділи:

1. Департамент охорони державної таємниці, технічного та криптографічного захисту інформації, про який вже йшлося вище. Зазначений орган здійснює контроль за станом забезпечення охорони державної таємниці, технічного та криптографічного захисту інформації в органах ДФС України.

Департамент виконує такі функції: контроль за дотриманням охорони державної таємниці в ДФС України та її територіальних органах; забезпечення технічного захисту інформації та організація криптографічного захисту інформації з обмеженим доступом, контроль за їх станом; організаційне керування комплексною системою захисту інформації в інформаційно-телекомунікаційних системах (автоматизованих системах) та здійснення контролю за її функціонуванням; організація моніторингу захищеності інформації та антивірусного захисту інформації в інформаційно-телекомунікаційних системах.

2. Департамент інформаційних технологій, відповідно до своїх повноважень, здійснює виконання в органах ДФС національної політики у галузі інформаційних технологій; розробляє програмні забезпечення та впроваджує інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи і технології, електронні сервіси для підприємців у державній митній та податковій справах, організовує їх технічне супроводження; організовує формування реєстрів, банків, баз даних та їхнє ведення; забезпечує функціонування документообігу та обміну інформацією з органами державної влади, державними органами іноземних держав, зокрема, митними та правоохоронними; реалізує інформаційно-аналітичне забезпечення органів ДФС та забезпечує автоматизацію її діяльності.

Крім того, цей Департамент виконує такі функції для забезпечення інформаційної безпеки органів ДФС:

– здійснює ведення Єдиного банку даних про платників податків – юридичних осіб та інших реєстрів, функціонування яких покладено на органи ДФС;

– забезпечує інформаційно-телекомунікаційні системи органів ДФС комп'ютерною технікою, системним та офісним програмним забезпеченням;

– забезпечує належну роботу електронних сервісів, їх технічну підтримку;

– наглядає за функціонуванням Єдиної автоматизованої інформаційної системи митного блоку органів ДФС;

– забезпечення використання електронного цифрового підпису в органах ДФС;

– організовує міжвідомчу взаємодію із суб'єктами інформаційних відносин щодо інформації про платників податків, об'єкти оподаткування та об'єкти, пов'язані з оподаткуванням;

– організовує роботу, пов'язану із захистом персональних даних фізичних та юридичних осіб при їх обробці.

3. Департамент обслуговування платників здійснює облік платників податків, зборів та обов'язкових платежів, а також ведення Державного реєстру фізичних осіб – платників податків, Єдиного реєстру податкових накладних, реєстру страхувальників, інших реєстрів та баз даних; організовує доступ до публічної інформації, роботи з приймання звітності платників податків; забезпечує впровадження електронних сервісів для підприємців.

Відповідно до покладених повноважень Департамент виконує такі функції:

– організовує і контролює порядок реєстрації та обліку платників податків;

– організовує взаємодію між учасниками інформаційних відносин щодо інформації про платників податків;

– забезпечує реалізацію робіт із приймання податкової, іншої звітності та її комп'ютерну обробку, а також приймає таку звітність засобами телекомунікацій;

– забезпечує захист персональних даних платників податків;

– організовує функціонування системи електронного адміністрування податку на додану вартість.

4. Департамент моніторингу доходів та обліково-звітних систем є підрозділом ДФС з координації діяльності органів ДФС для виконання всіх етапів бюджетного процесу, забезпечує інформаційно-аналітичне забезпечення керівництва органів ДФС, державних органів щодо діяльності з наповнення бюджту. У частині забезпечення інформаційної безпеки органів ДФС цей Департамент виконує такі функції:

– здійснює організацію ведення обліку податків, зборів, митних платежів тощо;

– контролює роботу підрозділів ДФС стосовно унеможливлення використання підприємцями інструментів з мінімізації сплати податків і зборів, у тому числі щодо виявлення несанкціонованого втручання в роботу інформаційних систем ДФС.

5. Головне управління внутрішньої безпеки, основними завданнями і функціями якого є:

– організація заходів із запобігання корупції та контроль за їх реалізацією в органах ДФС, її територіальних підрозділах;

– надання посадовим особам органів ДФС роз'яснень відносно дотримання положень антикорупційного законодавства;

– розгляд звернень громадян, їх об'єднань, суб'єктів господарювання стосовно можливих або вчинених корупційних, пов'язаних з корупцією або других порушень у галузі службової діяльності посадових осіб органів ДФС.

Загальними основними функціями підрозділів ДФС, які забезпечують інформаційну безпеку служби є:

– підготовка проектів нормативно-правових актів щодо забезпечення інформаційної безпеки держави, зокрема органів ДФС України;

– гарантування прав та свобод громадян, громадських об'єднань в інформаційній сфері;

– забезпечення у межах наданих повноважень вільного обміну інформацією з урахуванням встановлених законодавством обмежень на поширення інформації;

– моніторинг інформаційної безпеки органів ДФС України, аналіз її стану, виявлення внутрішніх, зовнішніх небезпек та загроз, а також джерел їх походження;

– розгляд пріоритетних способів попередження, нейтралізації, локалізації загроз, а також ліквідація їх негативних наслідків;

– протидія загрозам, які зазіхають на конституційні права особистості, суспільства і держави в інформаційній галузі;

– впровадження і розвиток інформаційної інфраструктури органів ДФС, а також виробництво інформаційних засобів у податковій й митній сферах діяльності;

– організація розробки загальнодержавних та відомчих концепцій щодо організації забезпечення інформаційної безпеки;

– організація здійснення наукових досліджень для забезпечення належного рівня інформаційної безпеки органів ДФС України;

– організація захисту інформаційних ресурсів органів ДФС;

– міжнародне співробітництво щодо виконання заходів інформаційної безпеки, представлення інтересів України у відповідних міжнародних організаціях [37].

Проаналізувавши обсяг повноважень Президента України, Верховної Ради України, Кабінету Міністрів України, Ради національної безпеки і оборони України, Служби безпеки України, Державної фіскальної служби України, інших державних органів, можна стверджувати, що завдання цих органів та служб мають обмежений склад комплексних рішень і функцій з питань забезпечення інформаційної безпеки в податковій та митній сферах життєдіяльності держави.

Такий підхід негативно впливає на інформаційну безпеку та якість відповідного захисту інформації, яка поширюється суб'єктами інформаційної взаємодії на об'єктах інформаційної діяльності та обробляється в інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних системах органів ДФС. Усе це може мати наслідком несанкціоноване поширення податкової й митної інформації та втручання у роботу відповідних інформаційних ресурсів. Також наявні внутрішні загрози інформаційній безпеці, які можуть проявляться з боку службових осіб органів ДФС.

Внутрішніми загрозами в інформаційній сфері органів ДФС є: несанкціоноване розголошення, поширення інформації з обмеженим доступом, яка стає відомою посадовим особам ДФС під час реалізації своїх повноважень; незаконне втручання до інформаційних систем, що призводить до зміни інформації та порушення встановленого порядку її маршрутизації, внаслідок чого зловмисники мають можливість використовувати таку інформацію для вчинення інших протиправних дій, зокрема ухилення від сплати податків, зборів тощо.

Для забезпечення високого рівня інформаційної безпеки органів ДФС, виявлення і протидії загрозам та правопорушенням, які вчиняються в інформаційній сфері, пропонуємо вдосконалити повноваження Головного управління внутрішньої безпеки ДФС для зменшення можливості вчинення несанкціонованих дій з інформацією посадовими особами Державної фіскальної служби під час адміністрування податків, зборів та платежів.

Для цього Департаменту інформаційних технологій потрібно доручити створити програмне забезпечення «Електронний журнал безпеки» в інформаційній системі (далі – ІС) «Податковий блок», за допомогою якого стане можливим фіксувати дії користувачів ІС «Податковий блок» та її інтегрованої автоматизованої системи «Перегляд результатів співставлення» під час вибірки даних у системі, а також дій під час відкриття та перегляду електронних документів.

Переглядати інформацію щодо користувачів матиме повноваження лише Головне управління внутрішньої безпеки ДФС. За допомогою підсистеми «Електронний журнал безпеки» стане можливим ідентифікувати осіб, які здійснюють несанкціоноване поширення інформації або спряють протиправному втручанню у роботу інформаційних систем.

Підсистема «Електронний журнал безпеки» має фіксувати дії користувачів ІС «Податковий блок» під час формування запиту до системи на вибірку податкових даних суб’єктів господарювання, а також дій під час відкриття та перегляду електронних документів.

При цьому формування даних у підсистемі «Електронний журнал безпеки» здійснюється лише на центральному рівні функціонування ІС «Податковий блок».

При перегляді «Електронного журналу безпеки» стане можливим здійснювати перегляд користувачів системи за такими окремими показниками: реєстраційний номер облікової картки платника податків – користувача ІС «Податковий блок»; прізвище, ім’я, по батькові працівника органу ДФС; ідентифікатор користувача; код органу ДФС; назва

режиму/підсистеми ІС «Податковий блок»; номер електронних данних (електронного документа), які переглядалися користувачем; дата та час дій; інформація щодо мережевого підключення (IP-адреси користувача).

У зв'язку з цим пропонуємо проект наказу ДФС «Про впровадження «Електронного журналу безпеки» в ІС «Податковий блок» (додаток А). У ньому необхідно виділити такі основні повноваження Головного управління внутрішньої безпеки ДФС:

– забезпечення реалізації заходів щодо запобігання корупції під час використання посадовими особами ІС «Податковий блок» в апараті ДФС, її територіальних органах за допомогю підсистеми «Електронний журнал безпеки»;

– здійснення методологічного супроводження складових підсистеми «Електронний журнал безпеки» в межах компетенції структурного підрозділу;

– за фактами виявлених причин і умов вчинення правопорушень під час роботи з ІС «Податковий блок» (несанкціоноване втручання у роботу інформаційної системи, незаконне розголошення інформації тощо) здійснювати підготовку пропозицій правового, соціального, економічного та організаційного характеру, спрямованих на запобігання та припинення таких правопорушень.

Отже, керуючись даними проведеного аналізу наукової літератури та законодавства, можна констатувати, що забезпечення інформаційної безпеки в діяльності органів ДФС України здійснюється внаслідок взаємодії досліджуваних державних органів з іншими суб'єктами, які є учасниками відносин у митній і податковій сферах.

Головними напрямами діяльності вказаних вище органів ДФС України, які здійснюють заходи щодо забезпечення інформаційної безпеки податкової й митної сфер держави, є: розробка законопроектів, забезпечення реалізації законних та підзаконних нормативних актів, що стосуються питань інформатизації в державі та її органів влади; створення організаційно-

правових засад для всебічного функціонування електронного документообігу, використання електронного цифрового підпису; сприяння розвитку технічних засобів збору та збереження інформації; формування, виконання програм криптографічного та технічного захисту інформації, виконання заходів державного контролю; здійснення заходів профілактичного характеру, спрямованих на гарантування інформаційної безпеки; проведення єдиної політики підвищення рівня інформатизації органів ДФС України; розвиток наявних та впровадження інноваційних автоматизованих технічних систем та програм в органах ДФС України; використання загальнодержавних довідкових та інформаційних баз даних; організація співпраці з міжнародними організаціями у сфері інформатизації.

## Висновки до розділу 1

На підставі викладених результатів дослідження основних питань розділу можна зробити такі висновки.

1. Сформульовано поняття: «митна інформація», «інформаційна безпека в діяльності органів ДФС України».

2. Для вироблення єдиного підходу щодо поняття «митна інформація» та усунення суперечностей щодо порядку її використання й зберігання органами ДФС запропоновано зазначене поняття чітко закріпити в Законі України «Про інформацію», зокрема у ст. 10, та окремо визначити у статті в такій редакції: «Митна інформація – це коло відомостей і даних, що збирається, накопичується та використовується органами ДФС для реалізації державної митної політики».

3. Встановлено, що інформація відіграє важливу роль у процесі управління державою. При цьому збір, оброблення та систематизація інформації дозволяють чітко визначити цілі та засоби досягнення поставленої мети. Розробка відповідних механізмів включає в себе як

механізми збору, зберігання інформації, так і механізми захисту від несанкціонованого втручання в інформаційні бази даних. Основоположне значення має оперативність та якість збирання й оброблення інформації. Існує пряма залежність між швидкістю збирання, оброблення інформації та ефективністю прийнятих і реалізованих управлінських рішень. Тобто, чим більше опрацьовується інформації, тим більш тісними стають зв'язки між структурними підрозділами органів держаного управління та контролю, зокрема в органах ДФС, і тим більш якісно та глибоко вони впливають на суспільство.

4. Визначено, що в органах ДФС використання податкової й митної інформації розподіляється за режимом доступу на відкриту та інформацію з обмеженим доступом.

5. Інформаційна безпека в діяльності органів ДФС України – це стан захисту інформації, інформаційних технологій та інформаційних ресурсів, працівників служби, фізичних та юридичних осіб від неправомірних дій чи бездіяльності суб'єктів інформаційних відносин, за якого здійснюється попередження, виявлення та протидія інформаційним правопорушенням.

6. Встановлено, що інформаційна безпека України повинна реалізовуватися практичними заходами відповідної державної політики у цій галузі внаслідок: гарантування, дотримання й забезпечення реальних прав і свобод кожної особистості, в тому числі в площині забезпечення права на отримання і використання інформації; формування інформаційної політики, яка б враховувала інтереси всіх верств населення та була доступною як на території України, так і поза її межами; створення стратегії інформаційного захисту, механізмів реалізації цієї політики через розвиток потужних інформаційних систем й елементів.

7. Важливим елементом державної політики розвитку податкової й митної систем країни є забезпечення інформаційної безпеки. Така політика

повинна забезпечувати відповідні гарантії безпеки інформаційних ресурсів та технологій, які використовують державні органи, зокрема ДФС.

8. Констатовано, що головним завданням органів ДФС України щодо забезпечення інформаційної безпеки є дотримання безпеки комбінацій доступу до інформаційних систем, цілісності та конфіденційності інформації, яка в них міститься.

9. Інформаційна політика органів ДФС визначається, як сукупність дій і заходів, спрямованих на дотримання й задоволення інформаційних прав, основних свобод фізичних та юридичних осіб внаслідок розробки, створення та забезпечення функціонування інформаційних систем і технологій, їхню інтеграцію у світове інформаційне середовище при гарантуванні інформаційної безпеки.

10. Суб'єктами забезпечення інформаційної безпеки в діяльності органів ДФС України є: Департамент охорони державної таємниці, технічного та криптографічного захисту інформації, Департамент інформаційних технологій, Департамент обслуговування платників, Департамент моніторингу доходів та обліково-звітних систем, Головне управління внутрішньої безпеки. Доведено, що завдання цих органів потребують вдосконалення з питань забезпечення інформаційної безпеки в податковій та митній сферах життєдіяльності держави.

11. Головними напрямами діяльності зазначених суб'єктів, що забезпечують інформаційну безпеку в органах ДФС України, є: розробка законопроектів, забезпечення реалізації законних та підзаконних нормативних актів, що стосуються питань інформатизації в державі та її органів влади; створення організаційно-правових засад для всебічного функціонування електронного документообігу, використання електронного цифрового підпису; сприяння розвитку технічних засобів збору та збереження інформації; формування, виконання програм криптографічного та технічного захисту інформації, виконання заходів державного контролю; здійснення заходів профілактичного характеру, спрямованих на гарантування

інформаційної безпеки; проведення єдиної політики підвищення рівня інформатизації органів ДФС України; розвиток наявних та впровадження інноваційних автоматизованих технічних систем та програм в органах ДФС України; використання загальнодержавних довідкових та інформаційних баз даних; організація співпраці з міжнародними організаціями у сфері інформатизації.

12. Запропоновано вдосконалити повноваження Головного управління внутрішньої безпеки ДФС України щодо виявлення і протидії інформаційним правопорушенням й розробити в інформаційній системі «Податковий блок» підсистему «Електронний журнал безпеки», метою якого є зменшення можливості вчинення несанкціонованих дій з інформацією посадовими особами ДФС України під час адміністрування податків, зборів та платежів.

13. Запропоновано проект наказу ДФС «Про впровадження «Електронного журналу безпеки» в ІС «Податковий блок».

# РОЗДІЛ 2

# ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

## 2.1. Інформаційне забезпечення процесу управління діяльності органів ДФС України

З урахуванням безупинного формування інформаційного простору в Україні постійно відбувається удосконалення механізмів отримання, накопичення, аналізу, розподілу та пошуку відповідної інформації. Це дозволяє співробітникам ДФС України більш якісно та ефективно виконувати свої службові обов'язки.

Законом України «Про Концепцію Національної програми інформатизації» виокремлено такі напрями інформатизації в державі:

1. Організаційно-правове супроводження інформатизації, що передбачає заходи стосовно розроблення нормативно-правових актів для правового регулювання відносин у цій сфері.

2. Розвиток державної структури інформатизації, що включає: міжнародні й міжміські телекомунікаційні і комп'ютерні мережі; систему інформаційно-аналітичних центрів різного рівня; інформаційні ресурси; інформаційні технології; систему науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації; системи підготовки висококваліфікованих фахівців у сфері інформатизації.

3. Інформатизація стратегічних напрямів державної діяльності, безпеки, оборони, що забезпечується процесом створення і розвитку інформаційно-аналітичних, обчислювальних та автоматизованих систем, центрів і мереж,

які забезпечують роботу державних органів й органів місцевого самоврядування.

Крім того, об’єктами інформаційної безпеки таких стратегічних напрямів державної діяльності є: канали інформаційного обміну, телекомунікації, інформаційні ресурси, механізми функціонування телекомунікаційних систем і мереж й інші елементи інформаційної інфраструктури держави.

4. Інформатизація процесів соціально-економічного розвитку та пріоритетних галузей економіки.

5. Інформатизація фінансової та грошової систем, державного фінансово-економічного контролю.

7. Інформатизація соціальної сфери.

8. Інформатизація в галузі екології та використання природних ресурсів.

9. Інформатизація науки, освіти і культури.

10. Міжнародне співробітництво. Зазначений напрям передбачає участь України в реалізації міжнародних проектів, в основу яких покладено формування умов для входження до глобальних інформаційних систем, захист національних інтересів при виконанні цих проектів та реалізацію стратегічних цілей державної зовнішньої політики [12].

Органи державної влади, керуючись своїми повноваженнями та в межах наданої компетенції, здійснюють такі завдання в сфері інформатизації: дотримання прав громадян, громадських об’єднань щодо доступу до інформації державних органів та органів місцевого самоврядування, враховуючи й інші джерела інформації; забезпечення захисту особистої інформації, авторських прав на інформаційні системи та програми, створені з метою інформатизації; виокремлення першочергових шляхів інформатизації та її підтримка, що забезпечується державним фінансуванням та пільговим оподаткуванням; встановлення та дотримання певних норм, правил та стандартів щодо напрямів використання засобів інформатизації;

інформатизацію державного управління, національної безпеки України, галузей економіки; забезпечення національного виробництва технічних, програмних засобів інформатизації; підготовка кваліфікованих вітчизняних спеціалістів у сфері інформатизації й інформаційних технологій; сертифікація засобів інформатизації; підтримка базових та фундаментальних теоретичних й практичних досліджень з метою проектування швидкісних засобів обробки та опрацювання інформації; забезпечення заходів інформаційної безпеки країни [32].

Інформаційне забезпечення дозволить інформаційним системам та ресурсам постійно вдосконалюватися й правильно функціонувати, досягати поставлених цілей щодо продуктивного управління потрібною діяльністю, а також є одним з найважливіших завдань органів державної влади.

У зв'язку з розвитком інформаційних технологій та комп'ютерних систем, інформаційне забезпечення відіграє важливу роль у дотриманні й гарантуванні інформаційної безпеки в діяльності органів ДФС України. Відповідно для досягнення цієї мети потрібно використовувати необхідний для такої ситуації комплекс методів комп'ютерної обробки даних, що допоможе збирати податкові чи митні дані для подальшого їх використання та аналітичних досліджень, аналізу, та, що найважливіше, прийняття рішень оранами ДФС.

Інформаційне забезпечення органів ДФС дозволить проводити своєчасний комплексний оперативний аналіз інформаційних матеріалів у податковій та митній сферах держави.

Проаналізувавши практику діяльності органів ДФС, можемо стверджувати, що інформаційне забезпечення є необхідною складовою податкової й митної справ, адже забезпечує найкращу продуктивність роботи. Ефективність полягає у тому, що ця система забезпечує здійснення усієї службової діяльності ДФС, у тому числі збирання, опрацювання та зберігання усіх видів інформації: багатоцільової, статичної, аналітичної, довідкової.

На сьогодні науковці та практики здебільшого використовують кілька підходів щодо визначення інформаційного забезпечення в діяльності органів ДФС України.

Досліджуючи інформаційне забезпечення органів Державної податкової служби, Стаценко-Сургучова І.С. зазначає, що категорія «забезпечення» часто вживається в законодавстві, юридичній та науковій літературі у сполученні з новими прикметниками чи самостійно, наприклад, при розгляді питань правового регулювання окремих видів діяльності або уповноважених суб'єктів чи методичних, теоретичних, процесуальних основ використання наукових методів, технічних засобів і інших мовних ситуацій без відповідних пояснень [144, с. 29].

Єдиним нормативним документом, в якому роз'яснюється поняття «інформаційне забезпечення», є ГОСТ 34.003-90 «Державний стандарт СРСР: Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Автоматизовані системи. Терміни і визначення», введений у дію 01.01.1992 р. [84].

Вказаний документ визначає інформаційне забезпечення як сукупність документів за формою нормативної законодавчої бази та рішень, реалізованих відносно розмірів, розташування і форм існування інформації, що застосовується в інформаційній системі при її використанні. Однак зазначений документ був розроблений ще за часів СРСР. У звязку з цим можна констатувати, що на сьогодні законодавець не приділяє достатньої уваги питанню інформаційного забезпечення, тому що нормативно-правові документи щодо формування інформаційного середовища різних сфер людської діяльності, в тому числі такого, яке стосується митної й податкової сфер, не приймаються.

Науковці, які досліджують окремі моменти інформаційного забезпечення, пропонують своє розуміння цієї категорії. Так, Стокороса Т. М. визначає інформаційне забезпечення як динамічну систему щодо одержання, зберігання, оцінки та переробки даних, яка створена з метою вирішення

управлінських рішень. Він також розглядає інформаційне забезпечення і як процес, і як сукупність документів, нормативно-правової бази, виконаних рішень стосовно розміщення й форми існування інформації, яка циркулює в інформаційній системі в ході її функціонування [147, с. 299].

Плішкін В.М. зазначає, що інформаційне забезпечення можна розглядати, як комплекс технічних, організаційних, технологічних і правових заходів, засобів й методів, які здійснюють підтримання у системі управління та під час її функціонування інформаційні зв'язки елементів (об'єктів, суб'єктів) через оптимальну організацію інформаційних баз даних і знань [125, с. 531].

У теорії управління під інформаційним забезпеченням розуміють діяльність, що організовується в рамках управління, спрямовану на проектування, запровадження й функціонування інформаційних систем, що дозволить ефективно вирішити завдання управління [70, с. 21].

Косиця О.О. визначила інформаційне забезпечення адміністративної діяльності під час адміністрування податків, зборів як встановлену діяльність фіскальних органів, а також інших публічних органів державної влади та фізичних і юридичних осіб щодо збору, опрацювання, зберігання та захисту інформації, яку використовують для внутрішньої та зовнішньої організації діяльності фіскальних органів [95, с. 71].

Блищик Л. П. розглядає інформаційне забезпечення діяльності ДФС України як динамічний процес одержання, зберігання, оцінки й переробки учасниками податкових правовідносин відомостей, які потрібні їм для реалізації власних прав та обов'язків у сфері оподаткування та які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [66, с. 165].

Інформаційне забезпечення управління в діяльності органів ДФС України включає всі сходинки управлінського циклу, а саме від підготовки, прийняття рішення до організації виконання і контролю результатів. Воно містить: збір елементарної інформації про керовані системи та зовнішнє

інформаційне середовище; передачу цієї інформації каналами зв'язку до місця її обробки; обробку елементарної інформації для організації керуючої дії; передачу інформації щодо керуючої дії; забезпечення контролю за її реалізацією [144, с. 29].

Ми погоджуємося із Стаценко-Сургучовою І. С., яка вважає, що інформаційне забезпечення Державної податкової служби України потрібно розглядати, як встановлену законодавством діяльність із застосуванням принципів, методів, способів, правил, схем та алгоритмів, за допомогою яких здійснюється пошук даних, їх збір, обробка, накопичення та зберігання, з метою надання своїм підрозділам необхідних даних у обсязі, достатньому для функціонування системи [144, с. 35].

У свою чергу, Теремецький В. І. інформаційне забезпечення визначає, як такий вид діяльності, що передбачає забезпечення когось або чогось конкретними засобами. Тому, на думку науковця, належний рівень управління податковою й митною системами держави напряму залежить від стану інформаційного забезпечення фіскальних органів [148, с. 50].

Під час дослідження інформаційного забезпечення органів ДФС було визначено його концепцію. На нашу думку, інформаційне забезпечення управління в органах ДФС України являє собою сукупність організаційних, правових та технічних заходів, що формують інформаційні зв'язки складових системи управління за допомогою упорядкування інформації, баз даних і знань.

Враховуючи модернізацію та вдосконалення діяльності органів ДФС України, збільшення кількості платників податків й зборів, дуже великим став потік інформації, що надходить до ДФС та її підрозділів, зросла кількість документів, щодо яких необхідне негайне реагування, обсяг інформації давно перейшов межу, коли прості засоби обробки інформації дозволяють оперативно та доброякісно її обробити. Обробити й опрацювати таку велику кількість інформації можливо за умови функціонування інформаційних систем. Інформаційна система ДФС України – організований

комплекс збирання, зберігання, накопичення, обробки, оновлення, пошуку, відображення та надання споживачам інформації, необхідної для ефективного управління [73, с. 157].

Виходячи із зазначеного вище, можна стверджувати, що основою раціональної роботи всієї системи податкової й митної сфер є системне інформаційне забезпечення діяльності ДФС України. Важливість інформаційного забезпечення у роботі органів ДФС України проявляється в тому, що інформаційне забезпечення передбачає наявність сукупності нормативно-правових актів та документів, прийнятих рішень щодо збирання, опрацювання та збереження інформації, що обробляється в автоматизованих інформаційних системах.

Враховуючи викладене, можемо визначити, що інформаційне забезпечення органів ДФС України здійснюється стосовно: організації електронного документообігу; накопичення та збереження податкової й митної інформації в інформаційних ресурсах, автоматизованих інформаційних системах; опрацювання податкової й митної інформації, зокрема звітності; формування електронної бази нормативних документів.

Головними принципами функціонування інформаційного забезпечення в ДФС є: достовірність та повнота податкової й митної інформації; дотримання контролю за своєчасністю сплати податків, зборів; захист від незаконного доступу до інформаційної системи ДФС; стандартизація та уніфікація інформаційної галузі у взаємодії підрозділів ДФС; мінімізація помилок опрацювання податкової й митної інформації. Від правильного інформаційного забезпечення органів ДФС залежить своєчасність та повнота поповнення державного бюджету, правильність сплати податків, зборів, своєчасність отримання податкової звітності та справедливість у правовідносинах з платниками податків і зборів [88, с. 123].

Отже, інформаційна інфраструктура ДФС України є різноманітною та розгалуженою. На неї впливають такі основні чинники: територіальна розгалуженість органів ДФС України; наявність широкого спектра носіїв

інформації; різноманітність інформації за видом та правовим режимом доступу, що циркулює в ДФС України; наявність великої кількості зовнішніх джерел інформації. Це сприяє взаємодії зовнішньої та внутрішньої систем ДФС, поширенню правовідносин, що виникають з приводу обігу службової інформації, завдяки розвитку інформаційних технологій. Проте, незважаючи на всі позитивні чинники, зовнішня система обміну та взаємодія зв'язків не до кінця утворена та потребує перетворень, що має стати пріоритетом діяльності ДФС.

На думку Розума О.М., інформаційне забезпечення – це інформаційна підтримка діяльності в боротьбі із злочинами у сфері оподаткування, яка відбувається внаслідок своєчасного залучення відповідних інформаційних масивів (отриманих з різних джерел), накопиченої в різних відомчих обліках, банках даних та в інших позавідомчих інформаційних системах [132, с. 256].

Вважаємо доцільно, характеризуючи інформаційне забезпечення, підтримати позицію науковців щодо його умовного поділу на інформаційно-аналітичне та інформаційно-довідкове забезпечення. Так, інформаційно-довідкове забезпечення – це один із напрямів діяльності органів ДФС щодо приймання та обробки певних податкових даних, а також виявлення, розкриття та розслідування податкових злочинів у процесі використання інформаційно-пошукових систем, різних видів обліків, відомчих та позавідомчих баз даних [133, с. 177].

Відповідно до ст. 71 ПК України, інформаційно-аналітичне забезпечення діяльності контролюючих органів – це комплекс заходів щодо збору, опрацювання та використання інформації, необхідної для виконання покладених на контролюючі органи функцій. Інформаційно-аналітичне забезпечення передбачає вдосконалення статистичного обліку і звітності фіскальних органів, інформування про стан, динаміку, структуру податкових злочинів, критеріїв оцінки ефективності діяльності підрозділів податкової міліції стосовно збору необхідної й достатньої інформації для ефективної

роботи у напрямі профілактики і прийняття відповідних управлінських рішень щодо запобігання податковій злочинності [5].

Інформаційно-аналітична робота при виявленні та розслідуванні злочинів у сфері оподаткування – це збирання, накопичення, інтегрування, зберігання, аналіз і систематизація орієнтуючої і доказової інформації в цілях прийняття оптимальних для конкретної ситуації кримінально-правових, кримінально-процесуальних, оперативних та тактичних рішень з метою забезпечення ефективного виявлення, викриття та розслідування податкових злочинів [134, с. 143].

Для протидії ухиленню від сплати податків, зборів в економічно розвинених країнах досить активно використовують методи непрямого визначення податкових зобов'язань платників податків. Однак у нашій державі немає визначеної законодавством методики донарахування податкових зобов'язань непрямими методами й залишаються недостатньо вивченими окремі питання щодо отримання інформації про фактичну підприємницьку діяльність суб'єкта господарювання, яка буде надавати вихідні дані для розрахунків. Тому Розум О.М., Безрученко В.С. визначили інформаційне забезпечення застосування непрямих методів у вирахуванні податкових зобов'язань як сукупність методів, процесів, програмних та апаратних засобів, призначених для збирання, обробки, зберігання, передачі інформації щодо сум податкових зобов'язань за оцінкою витрат платника податків, приросту його активів, кількості осіб, які перебувають з ним у відносинах найму, інших елементів податкових баз за допомогою інформації, одержаної з джерел інших, ніж звітність або первинні документи. Особливостями інформаційного забезпечення застосування непрямих методів у визначенні податкових зобов'язань, на думку науковців, є: неочевидність джерел інформації, фрагментарність інформаційних об'єктів, протидія з боку несумлінних платників виявленню об'єктивної інформації щодо господарської діяльності, не задекларованої у податковій звітності, складність документування такої інформації [135, с. 224].

Методичними рекомендаціями визначення сум податкових зобов'язань непрямими методами, затверджених наказом ДПА України від 5 липня 2002 р. № 312 [50], передбачено, що в Україні можуть бути застосовані такі непрямі методи: економічного аналізу; розрахунку грошових надходжень; контролю витрат і доходів суб'єктів підприємницької діяльності – фізичних осіб; аналізу інформації про доходи і витрати платника податків.

Також для збирання та накопичення необхідної інформації органи ДФС можуть проводити інформаційно-аналітичну розвідку, яка становить собою процес отримання нової, своєчасної інформації про об'єкт, предмет чи явище, що становить оперативний інтерес на основі методів роботи з елементами інформації про певні факти та події. Аналітична розвідка фіскальних органів може проводитись у різних напрямах: робота з банками та базами даних як обласного, так і центрального рівня, й інших міністерств, органів та відомств; вивчення та використання програмних інструментів та комплексів, необхідних для роботи з інформаційними системами; застосування сучасних методів аналізу отриманої інформації з метою виділення необхідних елементів [132, с. 257].

Інформаційне забезпечення має великий вплив на належну організацію роботи інформаційних систем органів ДФС України. Інформаційна система – це сукупність дій щодо збирання, зберігання, накопичення, обробки, оновлення, пошуку, відображення та надання споживачам необхідної інформації. Основними елементами інформаційно-аналітичної системи органів ДФС є бази даних; системи обробки даних; автоматизовані робочі місця, які здійснюють свою працю на базі сучасних інформаційних технологій [88, с. 142].

Одними із функцій органів ДФС України, відповідно до ст. 19-1 ПК України, є прогнозування, аналіз надходжень податків, зборів, платежів, визначених Податковим та Митним кодексами України, Законом України «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування», джерела податкових надходжень, вивчення впливу

макроекономічних показників, законодавства, угод про вступ до міжнародних організацій, інших міжнародних договорів України на надходження податків, зборів, платежів, розроблення пропозицій щодо збільшення їх обсягу та зменшення втрат бюджету; забезпечення розвитку, впровадження та технічного супроводження інформаційно-телекомунікаційних систем і технологій, автоматизацію процедур, зокрема, контроль за повнотою та правильністю виконання митних формальностей, організація впровадження електронних сервісів для суб'єктів господарювання; надання консультацій відповідно до ПК України, законодавства з питань сплати єдиного внеску та інформаційно-довідкових послуг з питань оподаткування й іншого законодавства, контроль за додержанням якого покладено на контролюючі органи [5].

Крім того, відповідно до ст. 19, ст. 20 МК України митні органи інформують заінтересованих осіб про митні правила, про інформацію щодо законодавства України з питань державної митної справи у встановленому законом порядку. Статтею 21 МК України передбачено, що митні органи безоплатно надають консультації за зверненням підприємств та громадян з питань практичного застосування окремих норм законодавства України з питань державної митної справи [6].

Отже, головними напрямами вдосконалення інформаційного забезпечення управління в органах ДФС України є:

– організація захисту органами ДФС конфіденційної інформації про фізичних та юридичних осіб з метою недопущення несанкціонованого розповсюдження такої інформації, а також забезпечення високого рівня адміністрування податків, зборів, обов'язкових платежів;

– розробці спеціальних програмних комплексів для виявлення та протидії несанкціонованому втручанню до інформаційно-телекомунікаційних систем органів ДФС;

– здійсненні систематичного аналізу податкових та митних ризиків, що можуть бути пов'язані із здійсненням несанкціонованого втручання в роботу

автоматизованих систем ДФС України з метою оперативного реагування та координації діяльності структурних підрозділів з їх відпрацювання;

– виконанні аналітичної роботи відповідними підрозділами ДФС для визначення фактів протиправної діяльності у податковій та митній сферах;

– проведенні митних процедур з використанням інформаційних систем і засобів їх забезпечення.

Підсумовуючи, можна констатувати, що на сьогодні маємо значні кроки в питаннях створення ефективних, професійних, розвинутих в інформаційному плані органів ДФС. Розвиток таких засобів та цілей наближає ці органи при впровадженні відповідної діяльності до європейських та міжнародних стандартів, що в перспективі повинно суттєво зменшити витрати часу та державні кошти та мінімізувати влив людського фактору на процедуру прийняття рішень.

Отже, інформаційне забезпечення процесу управління діяльністю органів ДФС України становить собою організаційні, правові, технічні заходи, які здійснюють формування інформаційних зв'язків складових системи управління на основі оптимальної організації інформації, баз даних і знань.

## 2.2. Інформаційні відносини та організація захисту інформації в органах ДФС України

Поширення інформаційних відносин є процесом об'єктивним, що, у свою чергу, супроводжується також і розвитком інформаційних технологій. У зв'зку з цим виникає необхідність у відповідному юридичному врегулюванні таких інформаційних відносин.

Розгляд проблемних питань регулювання інформаційних відносин, визначення їх безпеки в податковій та митній сферах зумовлюється необхідністю гарантування законних прав та інтересів їх суб'єктів, що

дозволить підвищити рівень взаєморозуміння між органами ДФС України та платниками податків, зборів, а також результативності виявлення нових незаконних схем у підприємницькій діяльності [158, с. 143].

Основні принципи здійснення інформаційних відносин в Україні юридично закріплено в ст. 2 Закону України «Про інформацію» [22], а саме:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

– правомірність одержання, використання, поширення, зберігання та захисту інформації;

– захищеність особи від втручання в її особисте та сімейне життя.

Проте до сьогодні поняття інформаційних відносин не має свого законодавчого визначення.

Як відомо, адміністративно-правові відносини виникають, розвиваються та припиняються між публічними органами державної влади та між ними і фізичними, юридичними особами. Можна сказати, що інформаційні відносини, які виникають між органами ДФС та органами державної влади, фізичними та юридичними особами щодо одержання, використання, поширення та зберігання різноманітної інформації є адміністративно-правовими [154, с. 54].

Проаналізуємо підходи науковців до розуміння інформаційних відносин, які врегульовуються нормами права.

У своїх дослідженнях Швець М. Я., Калюжний Р. А., Цимбалюк В. С. визначають інформаційні правовідносини як суспільні відносини щодо інформації, що є основним об’єктом регулювання інформаційного права. Цимбалюк В.С. схиляється до необхідності сформувати систему особливого інституту суб’єктів інформаційного права у складі загальної частини теорії права з екстраполяцією на особливі правові інститути суб’єктів (людини, громадянина, суспільства, держави) в особливій частині та за учасниками

видів інформаційної діяльності. До спеціальних родових ознак суб'єктів інформаційного права він пропонує віднести таких учасників інформаційної діяльності, які мають назву: інформатор – той, хто інформує, та інформований – той, хто отримав інформацію [160, с. 88].

На думку Рассолова М.М., інформаційно-правові відносини, або інформаційні правовідносини – це такі відносини, що виникають між різними учасниками (громадянами, редакціями газет, телестудіями, підприємствами, організаціями, фірмами тощо), в яких вони наділені правами і обов'язками, встановленими нормами інформаційного права [129, с. 42].

У свою чергу, Брижко В. М., Кальченко О. М. та інші кваліфікують їх як відносини, які мають місце у всіх сферах життя і діяльності людини, суспільства та держави при одержанні, використанні, поширенні та зберіганні інформації [68,с. 86]. Бачило І.Л. під інформаційними правовідносинами розуміє суспільні відносини, які виникають у процесі інформаційної діяльності [60, с. 22].

Туманова Л.В. та Снитников А.А. характеризують інформаційні правовідносини як суспільні відносини, що виникають згідно з нормами права та юридичних фактів при використанні інформаційних ресурсів на основі створення, збору, обробки, накопичення, зберігання, пошуку, поширення і надання споживачу документованої інформації; створенні і використанні інформаційних технологій і засобів забезпечення; захисту інформації, прав суб'єктів, які беруть участь в інформаційних процесах та інформатизації [143, с. 101].

Копилов В.А. інформаційні правовідносини розглядає, як врегульовані інформаційно-правовою нормою інформаційні суспільні відносини, в яких сторони виступають як носії взаємних прав і обов'язків, встановлених і гарантованих законодавством [92, с. 131]. До основних елементів інформаційних правовідносин, на його думку, належать: 1) суб'єкти, які вступають у правовідносини при здійсненні інформаційних процесів; 2) поведінка (дія, бездіяльність) суб'єктів при здійсненні ними інформаційних

правовідносин; 3) об'єкти, у зв'язку з якими суб'єкти вступають в інформаційні правовідносини; 4) право, обов'язок і відповідальність суб'єктів правовідносин при здійсненні інформаційних процесів. Він виділяє чотири групи таких відносин:

1) відносини, що виникають при здійсненні пошуку, отриманні і використанні інформації;

2) відносини, що виникають при створенні, передачі і поширенні інформації;

3) відносини, що виникають при створенні і застосуванні інформаційних систем, їх мереж, засобів забезпечення;

4) відносини, що виникають при створенні і застосуванні засобів і механізмів інформаційної безпеки [91, с. 131 – 132].

Кохановська О.В. аналізує інформаційні відносини за аналогією з правовими відносинами і визначає їх, як дії щодо збору, обробки і використання правової й іншої інформації в суспільстві. Такі інформаційні відносини характеризуються нормами права через сукупність специфічних ознак, до яких належать: наявність спеціальних суб'єктів інформаційної діяльності; наявність спеціальних об'єктів інформаційної діяльності (інформації, інформаційних технологій тощо); опосередкованість зазначених суб'єктів та об'єктів через інформаційні правовідносини. Науковець, аналізуючи світовий досвід законодавчого регулювання інформаційних правовідносин, виділяє такі їхні групи: право громадян на доступ до інформації, захист інформації, охорона виключних прав [96, с. 19].

На думку Яременко О.І., інформаційні правовідносини – це суспільні відносини, що регулюються нормами права і виникають, розвиваються та припиняють свою дію в інформаційному просторі між суб'єктами права, які наділені інформаційними правами та обов'язками. Під інформаційним простором, у свою чергу, учений розуміє інформаційні процеси та відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, обробки, захисту та поширення інформації, інформаційних

продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави [165, с. 158].

Інформаційні правовідносини Арістова І.В. розподіляє за такими критеріями:

– за галузевою сферою: конституційні, цивільні, адміністративні, трудові, екологічні тощо. На її думку, фактично всі галузі права включають сукупність норм, що регулюють інформаційні відносини в межах предмета певної галузі;

– за сферою поширення такі відносини можуть бути внутрішньо організаційні і зовнішні. Внутрішньоорганізаційні інформаційні відносини виникають і розвиваються під час здійснення внутрішньої діяльності державних органів, органів місцевого самоврядування, об'єднань громадян, господарських товариств, установ, організацій. У свою чергу, зовнішні правовідносини виникають між громадянами, об'єднаннями громадян, підприємствами, установами, організаціями та державними органами, органами місцевого самоврядування; між органами державної влади тощо;

– за тривалістю у часі такі відносини поділяють на постійні й тимчасові. Постійні інформаційні правовідносини виникають й розвиваються в будь-який час, їх тривалість та періодичність не обмежуються встановленими хронологічними рамками [56, с. 88].

Досліджуючи інформаційні правовідносини, Шпенов Д.Ю. визначив їх, як відносини, що мають місце у процесі здійснення інформаційної діяльності, що врегульована нормою права, а саме: виробництва, збирання, зберігання, перетворення, пошуку, отримання, поширення і споживання інформації, а також функціонування інформаційної інфраструктури. Виникають інформаційні правовідносини на підставі формально-юридичних передумов, до яких належать: норма права, право- та дієздатність суб'єктів, юридичний факт. Також вони розвиваються, припиняються при самостійному обороті інформації, при створенні і застосуванні автоматизованих інформаційних технологій, засобів і механізмів інформаційної безпеки [163, с. 7 – 9].

Гаврилов О.А. зауважує, що інформаційні правові відносини – це врегульовані правом відносини, в яких один суб'єкт (фізична або юридична особа) має право вимагати від іншого суб'єкта отримання певної інформації, а інший – зобов'язаний передати першому певний вид інформації [71, с. 52].

Монахів В.М. визначає інформаційні правовідносини, як відносини, що виникають у різних сферах суспільного та особистого життя у зв'язку з реєстрацією, збором, передачею, зберіганням і обробкою різних видів соціальної інформації. Після врегулювання правом вони відповідно стають інформаційними правовідносинами [110, с. 35 – 36].

Розглядаючи інформаційні відносини з позицій адміністративного права, Линник Г.М. визначив поняття «адміністративні правовідносини в інформаційній сфері», як суспільні відносини, що врегульовуються нормами адміністративного права та є специфічними, які виникають між суб'єктами адміністративних правовідносин під час одержання, використання, опрацювання, поширення й зберігання інформації. Як наслідок, між такими суб'єктами виникають взаємні права та юридичні обов'язки. Вказаним науковцем виокремлено основні характеристики адміністративних правовідносин в інформаційній сфері, зокрема такі: вони виникають, змінюються, припиняються тільки за умови наявності певної адміністративної норми; однією стороною правовідносин є юридично-владна особа, тобто державні органи, органи місцевого самоврядування, їхні службовці, а також інші суб'єкти, які виконують управлінські функції; наявність волі одного із суб'єктів адміністративного права; взаємні суб'єктивні права та юридичні обов'язки, що передбачені законодавством і забезпечуються державою; чітко врегульована, персоніфікована ознака взаємовідносин; сфера публічних правовідносин є сферою існування; виникають, припиняються або змінюються на підставі створення, одержання, поширення, використання та зберігання інформації; інформаційні права та законні вимоги людини і громадянина є пріоритетними у публічних

правовідносинах. В адміністративних правовідносинах інформаційна складова відіграє як вирішальну, так і допоміжну роль [100, с. 13].

Для інформаційних правовідносин, що реалізовуються у рамках права, характерні такі специфічні ознаки:

1) наявність спеціальних суб'єктів інформаційної діяльності держави, її органів, засобів масової інформації, підприємницьких структур, громадян;

2) наявність спеціальних об'єктів інформаційної діяльності, інформаційних інструментів (інформація, ресурси, інформаційні технології тощо);

3) опосередкованість та взаємозв'язок через інформаційні правовідносини вказаних суб'єктів і об'єктів [130, с. 29].

Досліджуючи питання правового регулювання відносин в інформаційній сфері, науковці зазначають про спроби законодавців створити інформаційну політику на базі демократичних норм і принципів, забезпечити їх адаптацію до умов розвитку нашої держави. Однак в умовах, коли немає загальнодержавної системи законодавства в інформаційній сфері правотворення в Україні часто здійснюється внаслідок фрагментарного вирішення наявних проблем в окремих законах та підзаконних нормативно-правових актах [163, с. 15].

Так, на етапі становлення інформаційного права, як галузі публічного права, за парадигмою фрагментарного підходу до юридичного врегулювання суспільних відносин щодо інформації сформувалася значна кількість нормативно-правових актів (понад 4000). Нині відчувається потреба в їх узгодженні. За умов подальшого розвитку інформаційного суспільства в Україні проблематика інформаційних правовідносин стає дедалі актуальнішою. Одним із її аспектів і є проблеми інкорпорації інформаційного законодавства України [165, с. 10].

Нині дослідники виділили такі завдання, які виникають перед державою в галузі інформації та інформаційних правовідносин:

1) гарантування й забезпечення розвитку, функціонування та захисту всіх форм власності на інформацію та інформаційні ресурси;

2) формування інформаційних систем і мереж як державного, так і регіонального рівня, що також передбачає вжиття організаційних й технічних заходів щодо забезпечення їхньої сумісності в єдиному інформаційному середовищі України;

3) дотримання стану захищеності державних та регіональних інформаційних ресурсів;

4) формування ринку інформаційних послуг, інформаційних систем, ресурсів та технологій, а також сприяння їхньому розвитку;

5) створення належних сприятливих умов для якісного інформаційного забезпечення людини і громадянина, органів державної влади, органів місцевого самоврядування, громадських об'єднань на базі інформаційних ресурсів держави;

6) вжиття заходів щодо забезпечення захисту інформації у галузі інформатизації, дотримання прав людини і громадянина в умовах інформатизації;

7) підтримка наукових програм і проектів у сфері інформатизації;

8) вироблення та реалізація єдиної технічної та промислової державної політики в галузі інформатизації, враховуючи сучасний міжнародний рівень розвитку інноваційних технологій;

9) створення та вдосконалення умов залучення інвестицій з метою стимулювання розробки й впровадження проектів інформатизації;

10) розвиток національного законодавства у галузі інформаційних процесів, інформатизації та захисту інформації з урахуванням провідного світового досвіду [152, с. 10].

Узагальнюючи зазначене вище, пропонуємо визначити інформаційні правовідносини в податковій та митній сферах як однорідну групу суспільних відносин, що виникають під час виконання покладених на органи ДФС функцій та завдань щодо справляння податків та зборів, здійснення

державної митної справи, а також щодо реалізації платниками податків і зборів права на податкову й митну інформацію.

Під структурою нормативного врегулювання інформаційних правовідносин, які мають місце в органах ДФС України, пропонуємо розуміти систему об'єднаних загальною ідеєю реалізації національних інформаційних інтересів, сукупність нормативно-правових актів, що врегульовують інформаційні правовідносини у податковій й митній сферах. Зміст структури такого нормативного врегулювання складають єдність, несуперечливість, системність, цілеспрямованість, узгодженість.

Концепція захисту інформаційних відносин у системі органів ДФС України, на думку Нестеренко О.В., має передбачати реалізацію технологій захисту інформації на всіх рівнях інформаційної системи та забезпечувати:

1) автентифікацію суб'єктів інформаційних відносин в органах ДФС України;

2) контроль доступу до об'єктів інформаційних відносин в органах ДФС України;

3) підтвердження цілісності документів із застосуванням електронного цифрового підпису;

4) захист інформації в ДФС України за допомогою засобів шифрування [114, с. 65].

Реалізація цих вимог значною мірою пов'язана із застосуванням засобів інфраструктури відкритих ключів (PKI). Використовуючи PKI, ДФС України забезпечує:

1) захист персональної (такої, що не класифікується) інформації й комунікацій – внутрішніх та зовнішніх;

2) захист конфіденційної та таємної інформації;

3) гарантії конфіденційності й ідентифікації, цілісності даних і автентичності [114, с. 65].

Основною метою захисту інформації та інформаційних відносин в органах ДФС України є недопущення нанесення матеріальної, фізичної,

моральної та іншої шкоди учасникам інформаційних правовідносин. Зазначена мета досягається завдяки забезпеченню та постійному підтриманню таких властивостей податкової й митної інформації: доступності інформації для зареєстрованих користувачів; збереження в таємниці визначених інформаційних ресурсів; цілісності та автентичності інформації, що зберігається, оброблюється та передається каналами зв'язку [112, с. 327].

Вважаємо, що захист інформації та інформаційних відносин в органах ДФС України є станом інформації, інформаційних ресурсів та інформаційних і телекомунікаційних систем, за якого з необхідною вірогідністю забезпечується безпека інформації в органах ДФС України.

Також захист інформації науковці розглядають, як стан захищеності інформації в органах ДФС України, що обробляється засобами обчислювальної техніки або автоматизованої системи від внутрішніх та зовнішніх загроз. Захист інформації забезпечується внаслідок недопущення несанкціонованого доступу до інформації, розкриття, модифікації або руйнування [81, с. 132].

Отже, нормативно-правове врегулювання захисту інформації, інформаційних відносин в органах державної влади, зокрема в органах ДФС, ґрунтується на основі адміністративно-правових принципів забезпечення захисту інформації, під якими можна визначити відправні начала, засади, ідеї, орієнтири, на підставі яких врегульовуються адміністративно-правові відносини.

Зокрема, такими адміністративно-правовими принципами є: верховенство права та закону; гласність; вільний доступ до інформації, відкритість інформації; заборона поширення інформації, яка є шкідливою або небезпечною для розвитку й функціонування державних чи недержавних правових інституцій, а також людини та громадянина; демократичність громадського контролю над державно-правовими інституціями; забезпечення прав громадян на участь у державному управлінні; чіткість розмежування

повноважень та дотримання взаємодії державних органів у забезпеченні інформаційної безпеки; пріоритет прав і свобод людини і громадянина в інформаційній сфері; своєчасність та обміркованість забезпечення державних інтересів в інформаційній галузі за допомогою керування потенційними та реальними загрозами; пріоритетність норм міжнародного права щодо національного законодавства; відповідальність посадових осіб державних органів за прийняті адміністративні рішення тощо [100, с. 12].

Олійник О.В. запропонував систематизувати принципи захисту інформації на правові й організаційні. До правових принципів захисту інформації він відносить принципи: законності; пріоритету норм міжнародного права над національним законодавством; права власності; економічної доцільності. До організаційних принципів захисту інформації – об'єктивності; наукового підходу до організації захисту інформації; комплексного підходу; безперервності захисту інформації; єдиноначальності; персональної відповідальності; централізовано-децентралізованого державного управління [118, с. 75].

Згідно з чинним законодавством України, захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Для її забезпечення державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством [13].

Об'єктом діяльності органів ДФС у такому випадку буде інформація, а також приміщення, в яких знаходяться автоматизовані системи, необхідні для роботи з інформацією.

Новицький А.М. стверджує, що дієвий захист інформації в податковій сфері при електронному оподаткуванні значною мірою залежить від належного організаційно-правового забезпечення, чіткого визначення прав і

обов'язків суб'єктів інформаційних відносин, завдань і повноважень організаційних структур щодо захисту інформації тощо [81, с. 146].

Попова С.М. вказує, що в українському законодавстві визначено, що будь-які інформаційні ресурси підлягають обов'язковому обліку та захисту [127].

Обов'язок встановлення та вибору режимів захисту інформаційних систем, у тому числі доступу до них, лежить на власникові цих ресурсів. Адже доступ до інформаційних процесів та великої кількості людей може сприяти «витоку інформації» та неправильному її використанню, що належить до негативних явищ.

До таких явищ можна віднести: численні порушення у фінансовій сфері, які призводять до ухилення від сплати податків, зборів, розтрати бюджетних коштів; несанкціонований доступ до інформації; неправочинні зміни, що спотворюють зміст інформації, внаслідок чого вона втрачає юридичну значущість і цінність; численні явища, що призводять до значних негативних наслідків як для окремих платників податків, зборів, так і в масштабах цілої країни [127, с. 274].

На думку Кормича Б.А., питання захисту найбільш значущої інформації та застосування обмежень щодо її функціонування та обігу можна цілком справедливо вважати найбільш давнім напрямом інформаційної безпеки держави. Від самого виникнення такого інституту, як держава, почала поширюватися практика оголошення різних відомостей таємними і встановлення відповідних правових норм для захисту цієї таємниці [93, с. 27].

Захист інформації в діяльності органів ДФС України пропонуємо розуміти, як сукупність дій, спрямованих на вжиття дієвих заходів забезпечення безпеки інформації, що функціонує в інформаційних та автоматизованих системах. Такі заходи, зокрема, включають у себе: протидію небажаному розголошенню (порушенню конфіденційності),

перекручуванню (порушенню цілісності), зниженню рівня доступності (порушенню доступності).

Основними реальними та потенційними потребами у захисті інформації, яка циркулює в органах ДФС України, є загроза розголошення інформації, що, згідно з законодавством, становить державну чи іншу, передбачену законом, таємницю, а також службової інформації, що є власністю органів ДФС та спрямована на гарантування її інтересів (зокрема конфіденційної інформації, що є власністю фізичних або юридичних осіб – платників податків, зборів). Крім того, порушення доступності, цілісності та спостережності інформаційних ресурсів.

На сьогоднішні державні органи здійснюють заходи щодо забезпечення зростання країни, в тому числі економічного, підтримку пріоритетних галузей економіки та реформування податкової й митної систем. Враховуючи такі обставини, виникає потреба у належному державному та правовому врегулюванні особливих економічних відносин, які виникли в умовах глобального розвитку інформаційних технологій, що впливає на провадження підприємництва інформаційних мереж.

Одним із таких важливих регуляторів виступає податковий та митний контроль, що зумовлюється, *по-перше*, розвитком інтернет-технологій, що використовуються суб'єктами господарювання для запровадження нових схем та способів ухилення від оподаткування, «відмивання» незаконно одержаних доходів, здійснення різноманітних махінацій з фінансовими ресурсами; *по-друге*, нагальною потребою розробити дієву систему державного регулювання сфери електронної комерції та належного механізму протидії податковим та фінансовим злочинам у цій сфері; *по-третє*, своєчасним нормативно-правовим забезпеченням підприємницької діяльності щодо використання інтернет-технологій [155, с. 150].

Важливим заходом захисту інформації в органах ДФС України є взаємодія інформаційних систем органів ДФС України з державними реєстрами. Наприклад, між Єдиним державним реєстром юридичних осіб та

фізичних осіб – підприємців (далі – Єдиний державний реєстр) і інформаційними системами ДФС України існує взаємодія. Такий процес передбачає обмін документами в електронній формі, що дозволяє забезпечити безпеку та захист інформації, яка передається, на досить високому рівні. Таку інформаційну взаємодію між вказаними системами забезпечують адміністратори Єдиного державного реєстру та ДФС України. У свою чергу, засоби криптографічного захисту інформації, які мають сертифікат відповідності чи позитивний експертний висновок за результатами проведення державної експертизи, застосовують для захисту інформації. В ході реалізації такої інформаційної взаємодії використовують інформаційні системи: Єдиний державний реєстр Міністерства юстиції України; Єдиний банк даних про платників податків – юридичних осіб, Реєстр самозайнятих осіб, що є складовою Державного реєстру фізичних осіб – платників податків, та реєстр страхувальників Державного реєстру загальнообов'язкового державного соціального страхування ДФС України (далі – реєстри ДФС України) [47].

Адміністратор Єдиного державного реєстру здійснює контроль і забезпечує передавання інформації при виконанні реєстраційних дій стосовно юридичних осіб та фізичних осіб – підприємців, у тому числі повідомлення державного реєстратора юридичних осіб та фізичних осіб – підприємців, а також документів в електронній формі, встановлених вимогами Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців», з Єдиного державного реєстру до реєстрів ДФС України у робочий час [47].

Інформація та документи в електронній формі передаються ДФС України з її реєстрів до Єдиного державного реєстру одночасно з аналізуванням та опрацюванням такої інформації в реєстрах Державної фіскальної служби України і отриманням відомостей про клас професійного ризику виробництва або зняттям з обліку платників податків, зборів в органах ДФС України чи підготовки в електронному вигляді документів,

передбачених Законом України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців» [19].

Водночас, ДФС України здійснює контроль за відомостями, які надійшли з Єдиного державного реєстру, щодо коректності використання реєстраційного номера облікової картки платника податків з Державного реєстру фізичних осіб – платників податків або серії та номера паспорта (для фізичних осіб, які за своїми релігійними переконаннями відмовилися прийняти реєстраційний номер облікової картки платника податків й повідомили про це відповідний орган ДФС), а також повноти заповнення реєстраційних карток [47].

Для захисту інформації, зокрема такої, яка циркулює та зберігається в інформаційних системах ДФС України, використовують комплексну систему захисту інформації.

Головним завданням комплексної системи захисту інформації є: унеможливлення витоку інформації технічними каналами, а саме каналами побічних електромагнітних випромінювань і наведень, акустично-електричними й іншими каналами, які виникають за умови впливу фізичних процесів під час функціонування засобів обробки інформації, та інших комунікацій й технічних засобів; виявлення, запобігання і протидія несанкціонованим діям з інформацією, у тому числі які вчиняються за допомогою комп’ютерних вірусів; захист від цілеспрямованого впливу на засоби обробки інформації, що здійснюється за допомогою формування сигналів та фізичних полів та може призвести до порушення її цілісності й незаконного блокування [39].

Сукупність організаційних та технічних заходів, спрямованих на попередження та реагування на загрози безпеці інформації в органах ДФС, утворюють цілісну систему захисту інформації в ДФС України. Цей термін має достатню кількість відомих тлумачень, зокрема в законодавстві України, які, на нашу думку, не суперечать один одному. У запропонованому визначенні зроблено акцент не на методах, засобах і заходах захисту

інформації в інформаційних системах від протиправного доступу, витоку інформації, силових впливів, а на більш широкій категорії – управлінні інформаційним захистом. Йдеться про процеси захисту інформації, про контроль їх відповідності загрозам, проміжок часу і реакцію на можливі інциденти виникнення загроз щодо захисту інформації.

Доцільно звернути увагу на те, що формулювання ефективності комплексної системи захисту інформації в органах Державної фіскальної служби України співвідноситься, насамперед, з поняттям ефективності процесів нейтралізації загроз безпеці інформації, які можуть виникати. Отже, основні елементи, які характеризують ефективність комплексної системи захисту інформації в органах ДФС, будуть якісні й кількісні оцінки меж безпеки інформації, що реалізуються шляхом застосування методів, засобів і заходів захисту інформації у рамках структури процесів управління інформаційною безпекою згідно з моделями загроз, які визначено.

Водночас, формулювання ефективності комплексної системи захисту інформації в органах ДФС України має в своєму складі й економічні сторони застосування методів, засобів і заходів захисту інформації, обмежені процесами управління інформаційною безпекою. Ознаками ефективності в такому разі будуть якісні й кількісні оцінки економічної ефективності комплексної системи захисту інформації.

Сам хід оцінки ефективності комплексної системи захисту інформації в органах ДФС включає в себе моделювання системи захисту, винайдення, відбір та застосування показників, критеріїв та методів оцінювання ефективності.

Концептуальний підхід до побудови комплексної системи захисту інформації в інформаційних системах ДФС України містить процедури:

– аналіз первинних даних на проектування, розроблення вимог до архітектури, базових технологій і їх реалізації в системі (формування загальних вимог у системи, розроблення політики безпеки, технічного

завдання на побудову комплексної системи захисту інформації в органах ДФС України);

– розроблення допустимих варіантів побудови, впровадження й експлуатації системи, їх порівняльного аналізу та прийняття оптимального рішення (проект комплексної системи захисту інформації). Тобто виникає завдання вибору інтегрального показника раціональності для прийняття оптимального рішення [56, с. 45].

Багатогранний підхід щодо захисту інформації в органах ДФС – це побудова системи захисту з оптимізацією усіх її складових, загальний рівень ефективності якої оцінюється через значення показників «найбільш слабкого ланцюга» за схемою – методи-засоби-заходи-система. Такий багатогранний підхід до захисту інформації в органах ДФС передбачає інтеграцію різних видів захисту інформації, ступінь і структура якої залежить від моделі загроз й ефективності кожного з можливих критеріїв для конкретного об’єкта захисту.

До головних концептуальних способів захисту інформації та інформаційних відносин в органах ДФС відносять: спеціальне діловодство; відповідний режим, який включає інженерний та технічний захист складових інформаційної діяльності; технічний, а також криптографічний захист інформації; голографічний захист носіїв інформації; організаційний та правовий захист інформації, виокремлюючи його як окремий вид захисту, який включає як необхідність/порядок/відповідальність, так і елементи інших видів (законодавчу базу окремих видів захисту інформації).

Отже, можна зробити висновок, що квінтесенція комплексного підходу до захисту інформації в органах ДФС являє собою якісний та дієвий процес нейтралізації можливих загроз безпеці інформації, яка стосується збору та адміністрування податків, зборів протягом її життєвого циклу через вдосконалення інтеграції найбільш ефективних методів, засобів та заходів захисту інформації протягом комплексної системи захисту інформації.

За результатами атестації або експертизи комплексу технічного захисту інформації, яку проводять для перевірки захисту інформаційної системи в органах ДФС України, визначається можливість циркулювання інформації в певній сфері, охорона якої забезпечується державою.

Відповідальність за забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи [116].

Визначення та проведення робіт щодо захисту інформації Державної фіскальної служби України в системі виконується службою захисту інформації, яка гарантує визначення вимог до захисту інформації, проектування, розробку і модернізацію системи захисту, а також здійснення робіт з її експлуатації та контролю за нормами захищеності інформації.

На сьогодні виокремилися два підходи до забезпечення захисту електронних систем: фрагментарний підхід, при якому здійснюється протидія суворо визначеним загрозам за певних умов (спеціалізовані антивірусні засоби, автономні засоби шифрування, тощо); комплексний підхід, який передбачає створення середовища обробки інформації, що об’єднує різноманітні (правові, організаційні, програмно-технічні) заходи для протидії загрозам. Комплексний підхід, як правило, використовують для захисту великих систем. Хоча часто і типові програмні засоби містять вбудовані засоби захисту інформації, але цього замало. Для гарантування безпеки інформаційних систем, прямо чи опосередковано пов’язаних з адміністративним управлінням, вживають такі заходи: фізичний захист комп’ютерних систем; регламентація технологічних процесів; регламентація роботи з конфіденційною інформацією; регламентація процедур резервування; регламентація внесення змін; регламентація роботи персоналу і користувачів; заходи контролю і спостереження [94, с. 134].

Щоб сформувати системний підхід до захисту інформації в органах ДФС, таку інформацію можна розділити на категорії:

а) важлива інформація, тобто інформація, необхідна для діяльності, процедура відновлення якої, у разі її знищення, неможлива або ж вимагає великих затрат, при цьому її помилкове застосування чи підробка призводить до великих втрат;

б) корисна інформація – інформація, яка необхідна для діяльності та яка може бути відновлена без суттевих втрат, при чому її зміна або знищення призводить до відносно невеликих втрат;

в) конфіденційна інформація – інформація, доступ до якої для частини робітників та інших осіб небажаний, оскільки може стати причиною виникнення матеріальних та моральних збитків;

в) відкрита інформація – інформація, до якої мають доступ усі охочі та яка є відкритою за своєю суттю.

Основним завданням захисту інформації та інформаційних відносин в органах ДФС України є забезпечення доступності, цілісності і конфіденційності інформації.

Такі принципи передбачають можливість своєчасно отримати необхідну інформаційну послугу, а також запобігання несанкціонованої відмови в отриманні інформації; запобігання несанкціонованої модифікації або руйнування інформації; запобігання несанкціонованому ознайомленню з інформацією [112, с. 328].

Комплекс дій із захисту інформації в органах ДФС виконують із використанням модулів: комплексної системи захисту інформації в інформаційних та телекомунікаційних системах та технологічного захисту інформації.

При цьому система захисту інформації в інформаційній та телекомунікаційній системах органів ДФС являє собою сукупність організаційних, інженерних та технічних заходів захисту інформації.

Комплекс технічного захисту являє собою сукупність дії із захисту інформації з обмеженим доступом від початку виходу по технічних каналах.

Крім того, необхідно приділяти пильну увагу питанням захищеності інформації в органах ДФС у сучасних умовах функціонування в державі електронного документообігу, що становить собою сукупність процесів щодо створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів. Такі процеси реалізовують використовуючи перевірку їх цілісності і в разі потреби підтверджуючи факт одержання цих документів. Учасники електронного документообігу, які здійснюють його на відповідних договірних засадах, самостійно визначають режим доступу до таких електронних документів і встановлюють для них спеціальну систему захисту [127, с. 277].

У свою чергу, електронний документ є документом, інформація в якому збережена у вигляді електронних даних, включаючи обов'язкові реквізити документа. Обов'язковим реквізитом електронного документа є електронний підпис, який використовують для ідентифікації автора та/або підписування електронного документа іншими учасниками електронного документообігу. Оригіналом електронного документа вважається примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора [11].

Надсилання та передача електронних документів виконується його автором чи представником в електронній формі з використанням інформаційних, телекомунікаційних засобів та систем або через надсилання електронних носіїв, на яких зафіксований відповідний документ.

Орган виконавчої влади відповідно до п. 3 Постанови Кабінету Міністрів України від 28 жовтня 2004 р. № 1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» здійснює електронний документообіг тільки за умови використання надійних засобів електронного цифрового підпису, що підтверджується сертифікатом відповідності або позитивним висновком за

результатами державної експертизи у сфері криптографічного захисту інформації, одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів у своїх працівників – підписувачів [40].

Електронний цифровий підпис є різновидом електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладають за допомогою особистого ключа та перевіряють за допомогою відкритого ключа [27].

Електронний цифровий підпис має своє призначення, як засіб забезпечення належної діяльності фізичних та юридичних осіб з використанням електронних документів. Електронний цифровий підпис використовують особи, якщо є учасниками електронного документообігу, задля ідентифікації особи, яка підписала цей документ та для підтвердження цілісності даних, надісланих в електронній формі.

Ми погоджуємось з Новицьким А.М., який визначив електронне оподаткування як нормативно-врегульовану, динамічну, економічно обґрунтовану й доцільну, синтезовану систему автоматизованого встановлення податкового зобов'язання, визначення податкової бази, обліку платників податків, підготовки й подачі електронної звітності та інших складових адміністрування податків з метою його упорядкування та вдосконалення, створення умов для подальшого перспективного розвитку інформаційних відносин у сфері оподаткування [81, с. 250].

На сьогодні органи ДФС забезпечують належні умови для ефективної інформаційної взаємодії з платниками податків, зборів, забезпечуючи прозорість й доступність надання послуг таким особам. Крім того, фіскальна служба активно допомагає, наприклад, при заповненні декларації про майновий стан і доходи в режимі on-line, при формуванні та надсиланні електронної податкової звітності.

Дослідники з питань інформаційного захисту пропонують виділити такі методи забезпечення захищеності інформації. До універсальних методів захисту інформації вони віднесли: метод регламентації процесів захисту інформації (з використанням нормативно-правових норм можна визначити умови щодо діяльності, пов'язаної з обігом інформації з обмеженим доступом); метод приховування інформації, що підлягає захисту (встановлення обмежень, тобто ступенів секретності та конфіденційності інформації); метод роздроблення інформації та процесів її обігу (полягає в наданні доступу до інформації з обмеженим доступом користувачам лише в частині інформації, яка безпосередньо необхідна для виконання покладених завдань); метод дезінформування (полягає у свідомому поширенні викривленої інформації стосовно певних питань); метод системного обліку інформації з обмеженим доступом і процесу її автоматизованої обробки; метод підвищення ефективності людського фактора у сфері захисту інформації; метод створення фізичних і технічних перешкод на шляху зловмисника до інформації, що захищається; метод колегіального контролю за додержанням режиму секретності або конфіденційності [116, с. 105].

У свою чергу, Ліпкан В.А. пропонує виділити такі методи забезпечення інформаційного захисту в органах ДФС України:

– однорівневі методи, які будуються за одним принципом управління інформаційного захисту;

– багаторівневі методи, які будуються на основі декількох принципів управління інформаційним захистом. При цьому окремі технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

– комплексні методи, що являють собою багаторівневі технології, об'єднані в єдину систему координаційними функціями на організаційному рівні з метою забезпечення інформаційного захисту, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

– інтегровані високоінтелектуальні методи, що являють собою багаторівневі, багатокомпонентні технології, побудовані на потужних автоматизованих інтелектуальних засобах з організаційним управлінням [101, с. 237].

На нашу думку, для запобігання та нейтралізації загроз інформаційній безпеці органів ДФС необхідно застосовувати базові методи, а саме: правові, програмно-технічні та організаційно-економічні.

Правові методи передбачають розроблення системи нормативних документів і положень, що регламентують інформаційні відносини в органах ДФС, керівних і нормативно-методичних документів щодо забезпечення захисту інформації та інформаційних відносин в органах ДФС.

Одне з найважливіших завдань полягає у формуванні законодавчої та нормативно-правової бази, яка б забезпечила відповідний захист інформації шляхом розподілу та використання персональної інформації, яка міститься в базах даних, для формування взаємовідносин між органами ДФС та платниками податків, зборів, гарантування основ визначеного соціального компромісу, створення сервісної фіскальної служби, яка б була орієнтована здебільшого на задоволення бізнесових та господарських інтересів, формування умов для становлення соціального партнерства як основи демократичного розвитку суспільства.

Світовий та історичний досвід свідчить про те, що країни, які не змогли своєчасно забезпечити національний інформаційний простір ефективними технологіями, сповільнювали свій економічний розвиток. І навпаки, країни з потужним інформаційним потенціалом швидко відновлювали свою роль у світовому розподілі сфер впливу. Тому наповнення національного інформаційного простору новітніми технологіями, що можуть значно підвищити як адекватність відображення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що, у свою чергу, визначає можливості захисту національних інтересів [102, с. 120].

Розвиток інформаційного суспільства нашої держави є сучасною глобальною тенденцією, яка веде до значних змін у державних відносинах та економіці країни. Це потребує ряду соціально-політичних рішень, що б відповідали швидким змінам в усіх сферах життєдіяльності, зокрема, в процесах підготовки та прийняття рішень, у змісті та формах державного управління, в уявленнях про права людини, національну та особисту безпеку, в оцінюванні стратегічних ресурсів. Нині система інформаційного захисту держави є взаємопов'язаними елементами загальної системи державного управління. Розвиток та впровадження в різні сфери життя суспільства новітніх інформаційних технологій забезпечує комфортність, але й нерідко несе певну небезпеку. Загальними, зокрема, є групи інформаційно-технічних небезпек:

– новий клас соціальних злочинів, спрямований проти особистості, суспільства, держави, заснований на використанні сучасної інформаційної технології;

– використання нових інформаційних технологій в політичних цілях;

– електронний контроль за життям, планами громадян, політичних організацій [128, с. 42].

Отже, під системою захисту інформації й інформаційних відносин в органах ДФС розуміється взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Для її створення необхідно вжити заходів захисту інформації, які мають сертифікат відповідності або експертний висновок з позитивним результатом у сфері технічного та/або криптографічного захисту інформації.

## 2.3. Управління інформаційними ресурсами в діяльності органів ДФС України

Суттєві зміни, які відбуваються у зв'язку з інформатизацією усіх сфер життя, призводять до високого рівня розвитку науки і технологій, цілеспрямованого зростання інформаційних відносин у всіх напрямах життя суспільства. Водночас підвищується і рівень усвідомлення кожним учасником названих відносин необхідності їх правового забезпечення, дотримання конституційно закріплених прав людини в процесі здійснення інформаційної діяльності й прагнення до формування не тільки вільного, але і безпечного інформаційного простору.

Інформація та інформаційні ресурси перетворилися на стратегічний ресурс економічного і науково-технологічного прогресу держави і на визначальний фактор успішної внутрішньої і зовнішньої політики держави.

Стрімкий розвиток інформатизації та модернізація всіх гілок влади України потребує більшої мобілізації щодо формування інформаційного простору всіх сфер управлінської діяльності, не є винятком і органи ДФС.

Зарубіжні вчені зазначають, що «інформація» перебуває у нашому розпорядженні, як інтелектуальний ресурс, що захищений або доступний тільки для використання певними колами користувачів, але все більше як відкритий ресурс. Знання, генероване завдяки окремим інформаціям і реалізоване завдяки новим комунікаційним механізмам і формам розповсюдження, безперечно, вважається «важелем» і мотором економічних, соціальних і культурних змін. За цими змінами одночасно приховані шанси і ризики; у зв'язку з цим вони вимагають правових відповідей, які з виникненням інформаційного суспільства пропонують закріпити за двома феноменами або відповідно факторами: швидким розвитком нової техніки, мас-медіа і послуг інформації і комунікації та поширеною лібералізацією, спрямованою проти надмірної державної монополії на ринках телекомунікації і телерадіо [87, с. 11].

Враховуючи це, на нашу думку, дії, які спрямовані на збирання й обробку інформації, її осмислення, в цілому можна назвати інформаційною діяльністю.

Інформаційна діяльність є процесом створення, використання, поширення, а також пошуку інформації. Вона має усі риси, характерні для соціальної діяльності: цілеспрямованість, предметність, упорядкованість. Проте потрібно враховувати, що інформаційна діяльність, утворюючи комплекс сфери виникнення, розвитку і припинення інформаційних правовідносин, має свої особливості. Суспільні відносини, урегульовані правом, не завжди є відносинами-процесами, тобто відносинами динамічними за своєю природою, наявні також і статичні відносини. Проте статичні правовідносини не є процесами. Наприклад, статичними є відносини, які виникають щодо обігу інформації, що являє собою особисту таємницю. Відносини в інформаційній сфері можуть бути як статичними, так і динамічними. Об’єктом статичних відносин є якесь явище або інформація, а динамічних – поведінка особистості щодо інформації.

Інформаційні правовідносини виникають з виданням нормативних і індивідуальних актів, тобто виникненням їх юридичних підстав, а також з наявністю необхідних умов для правомірних дій чи утримання від неправомірних дій їх суб’єктів [149, с. 265].

Нині діяльність органів державної влади, зокрема органів ДФС, спрямована на використання передових технологій для реалізації поставлених цілей їх діяльності, а також необхідність оптимізування та удосконалення власної управлінської діяльності. Основним напрямом покращення оптимізації їх функціонування є більш розширене використання інформаційних ресурсів, інформаційного забезпечення діяльності.

Інформаційні ресурси складають сукупність даних, які у загальному у своїй сукупності є інформацією, тому для того щоб об’єктивно правильно охарактеризувати поняття інформаційних ресурсів, потрібно з’ясувати

погляди науковців на визначення інформації та правове врегулювання цього визначення.

За тлумачним словником, слово «ресурси» походить від французького ressourse – допоміжні засоби (грошові кошти, цінності, запаси, можливості, джерела прибутків тощо) [108, с. 28].

У минулому столітті до ресурсів включали різні за видами, такі як: фізичні, людські, грошові, механічні та енергетичні. Наявність таких корисних ресурсів тепер становить необхідність у ефективній діяльності кожних сфер діяльності, що вважається гарантією процвітання.

Із кінця 70-х років XX ст. у наукове і практичне життя стало широко входити шосте поняття: інформаційні ресурси. Їх не можна розглядати як різновид інших – вони існують самостійно і мають власні унікальні властивості та велике суспільне значення і впливають на всі суспільні процеси.

На даний момент такі ресурси витіснили та практично замінили згадані вище та належать до найважливіших. Це відбулося завдяки тому, що їх наявність показує інтелектуальні багатства, економічну стабільність, політичну та військову міць. Вони є більше ніж просто необхідність – це основа будь-якої діяльності, яка полягає у їх виробленні, перетворенні та використанні.

Зважаючи на зазначене, розглянемо більш детально теоретичні аспекти визначення поняття інформаційних ресурсів. Закон України «Про Національну програму інформатизації» дає визначення окремому інформаційному ресурсу як сукупності документів в інформаційних системах (бібліотеках, архівах, банках даних тощо) [32].

Аблякимов Е.Е. виділяє три основні підходи до цього тлумачення. По-перше, це узагальнюючий підхід, за якого інформаційні ресурси розглядаються на основі етимологічного значення слова «ресурси» та як сукупність інформації, що має певну матеріальну цінність. Як правило, такий підхід використовують у різних програмних документах з питань розвитку

інформаційної сфери. По-друге, інформаційні ресурси можуть розглядатися як матеріалізована форма представлення інформації для окреслення просторової дії права, що регулює інформаційні відносини. Відповідно до цього підходу виділяються національні інформаційні ресурси, правові відносини щодо яких та їх правовий режим врегульовано нормами національного законодавства. По-третє, термін «інформаційні ресурси» використовують для позначення конкретних цілісних утворень – масивів документів, пов'язаних інформаційними системами, які виступають специфічним об'єктом правового регулювання та мають свій власний правовий режим [54, с. 71 – 72].

Інформаційні ресурси – це відомості, які отримують та накопичують у процесі розвитку науки та практичної діяльності людей і використовують у суспільному виробництві та управлінні [142, с. 242].

Узагальнюючи усі зазначені вище позиції, можна стверджувати, що інформаційні ресурси – це, з одного боку, – весь масив інформації, або інформація в загальному значенні, з іншого – матеріальне відображення інформації, яка виражається в конкретних її носіях.

У контексті сказаного необхідно погодитись з Арістовою І.В., яка інформаційні ресурси відносить до системи інформаційного простору. На її думку, головними компонентами інформаційного простору є:

1) інформаційні ресурси, зокрема архіви, бібліотеки, музейні сховища, бази та банки даних, системи депозитаріїв державних інформаційних ресурсів тощо;

2) інформаційно-телекомунікаційна інфраструктура, до складу якої входять розподілені за територіальною ознакою державні та корпоративні комп'ютерні мережі, телекомунікаційні мережі і системи загального або спеціального призначення, канали передачі даних, засоби управління інформаційними потоками; інформаційні, комп'ютерні та телекомунікаційні технології у вигляді базових, прикладних і забезпечувальних систем, засобів їх реалізації;

3) науковий та виробничий потенціал у сферах зв'язку, інформатики, телекомунікації, обчислювальної техніки, поширення й доступу до інформації. Зазначений компонент включає: організаційні структури, враховуючи кадри, які забезпечують функціонування й розвиток національної інформаційної інфраструктури; ринок інформаційних технологій, засобів зв'язку, інформатизації, інформаційних продуктів та послуг; систему взаємозв'язку інформаційного середовища України із міжнародними відкритими мережами; систему забезпечення інформаційної безпеки; систему засобів масової інформації; систему інформаційного законодавства [56, с. 106 - 107].

Сировой О.В. визначив поняття інформаційних ресурсів, як повний обсяг відомостей, отриманих з навколишнього середовища, створених у процесі певної діяльності знань, даних, зафіксованих на матеріальних носіях, систематизованих за певною ознакою чи критерієм та призначених для зберігання і суспільного користування як на виробництві, так і в управлінні [140, с. 22].

Сировой О.В. зазначає, що до складу управління національною інформаційною сферою входить система управління інформаційними ресурсами МВС України. Тому він виокремив такі складові системи управління інформаційними ресурсами, як:

– суб'єкт управління – це спільноти людей, які структурно окреслені та утворюють органи управління різних організаційних структур, зокрема інформаційних підрозділів;

– об'єкти управління, якими є інформаційні ресурси, в яких зберігаються масиви документів;

– прямі й зворотні зв'язки між об'єктом та суб'єктом управління. Такі зв'язки реалізуються за допомогою техніки управління: технічних засобів пошуку, зберігання, опрацювання інформації тощо [140, с. 47]. З подібним розподілом потрібно погодитись.

Партико З.В. визначає інформаційні ресурси науково-технічної інформації як систематизовану сукупність науково-технічної літератури, документації, зафіксованих на паперових чи інших носіях [119, с. 34].

Стаценко-Сургучова І.С. розглядає інформаційні ресурси органів Державної податкової служби України, як встановлену законодавством діяльність таких органів, під час якої використовують принципи, методи, способи, правила, схеми та алгоритми, за допомогою яких здійснюється пошук інформації, її збір, опрацювання, накопичення, зберігання. Ця діяльність спрямована на надання своїм підрозділам необхідної інформації для вирішення певної ситуації у обсязі, достатньому для функціонування системи [144, с. 176].

Важко визначити концепцію інформаційних ресурсів. Вони зберігають задокументовану інформацію, але не повною мірою, отже не доцільно називати їх сховищами задокументованої інформації. На нашу думку, поняття інформаційних ресурсів набагато ширше: вони являють собою складну систему знань, згадану вище інформацію та всю інформаційну систему, в тому числі оператори, що опрацьовують вихідну інформацію.

Найбільш прийнятним варіантом термінологічного визначення інформаційних ресурсів є такий: «Це окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази та банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять відомості і знання, зафіксовані на відповідних носіях інформації, є об’єктами права власності всіх суб’єктів України і мають споживчу вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо)» [120, с. 46].

Розрізняють такі основні особливості інформаційних ресурсів:

– інформаційні ресурси є практично невичерпними на відміну від інших видів ресурсів, наприклад матеріальних;

– у процесі використання інформаційні ресурси зберігаються і, можливо, навіть збільшуються;

– інформаційні ресурси можуть належно функціонувати тільки в поєднанні з іншими життєво важливими ресурсами, наприклад, досвідом, кваліфікацією, працею, технікою, сировиною, енергією тощо, які виступають рушійною силою;

– за допомогою використання інформаційних ресурсів здійснюється повторне виробництво знань. Тобто інформаційна взаємодія дає можливість отримувати нові знання ціною менших витрат, порівняно з витратами праці, енергії, часу на його пряме генерування;

– інформаційні ресурси створюються на підставі розумової і творчої праці;

– перетворення знань в інформаційні ресурси здійснюється на підставі кодування таких знань. Є активна і пасивна форми інформаційних ресурсів, які виступають як відчужувані знання, які стають повідомленнями. Наприклад, модель, програма, алгоритм, проект і особливо бази знань – це активні форми інформаційних ресурсів. Статті, книги, патенти є пасивними формами [123, с. 10].

Мацюк В.Я., досліджуючи питання управління інформаційними ресурсами в діяльності органів ДФС України, зазначав, що без інформаційних технологій неможливо налагодити ефективну взаємодію між владними структурами, а також належним чином підвищити ефективність та якість вироблення та прийняття рішення, вчасно виявити управлінську помилку. ДФС України зацікавлена у електронних інформаційних ресурсах, які пов’язані зі здійсненням підприємницької діяльності, в т. ч. реєстрація, ліцензування, патентування, сертифікація, створених міністерствами, відомствами, інформація яких є необхідною при розслідуванні правопорушень у сфері оподаткування. Невизначеність правової основи діяльності різних суб’єктів призводить до інформаційного монополізму окремих структур на відкриті інформаційні ресурси загального користування, на обмеження права доступу ДФС України до інформації, права на використання інформаційних ресурсів [109, с. 115].

Плішкін В.М. зазначає, що інформаційні ресурси – це комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, які забезпечують у процесі управління і функціонування системи інформаційні зв'язки її елементів (суб'єктів і об'єктів) унаслідок оптимальної організації інформаційних масивів баз даних і знань [125].

Інформація, яка циркулює у суспільстві, перетворюється на знання у тому випадку, якщо її сприймають, селекціонують, аналізують і зберігають суб'єкти та можуть використовувати у практичній цілеспрямованій діяльності. У випадку, коли інформація, отримана суб'єктом, не проходить шлях подібної обробки, вона не може бути використаною у майбутньому і тому не перетворюється на знання. Іншими словами, будь-які знання являють собою інформацію, але не вся інформація може перетворитися на знання [140, с. 19 – 20].

Ключовим аспектом функціонування інформаційних ресурсів у органах ДФС України є можливість отримувати, володіти та розпоряджатися податковою, митною та похідною від неї інформацією. Вона є базовою для функціонування органів ДФС України, адже до певної міри виражає сутність призначення самої служби і наповнює її діяльність певним змістом. Тільки наявність значимої для органів ДФС України інформації дозволяє виконувати в повному обсязі поставлені завдання та реалізовувати визначені в законодавстві повноваження. Інформація фактично є рушійною складовою діяльності. Завдання, які виконують інформаційні ресурси в управлінні ДФС України, виражаються в тому, що вони:

– є специфічною формою взаємозв'язку, взаємодії компонентів системи, а також системи в цілому з навколишнім середовищем;

– обслуговує всі рівні та функції управління – від підготовки та прийняття рішення до підведення підсумків виконання;

– є безпосередньою причиною, яка визначає вибір системною того чи іншого варіанта поведінки, переводу системи в новий стан, що забезпечує її рух до заданої мети [88, с. 77 – 78].

Важливим аспектом інформаційної діяльності органів ДФС є управління інформаційними ресурсами, про які йшлося вище. Сировой О.В. зазначає, що управління інформаційними ресурсами – діяльність суб'єкта управління щодо досягнення бажаного стану інформаційних ресурсів (об'єкта управління), внаслідок цілеспрямованого управлінського впливу, що здійснюється за допомогою організаційно-правових заходів та техніки управління, за схемою прямого та зворотного зв'язку з урахуванням вимог нормативно-правових актів для всебічного задоволення інформаційних потреб [140, с. 177].

У загальному вигляді під інформаційними ресурсами органів ДФС України розуміють комплекс інформації, що міститься у базах даних, електронних бібліотеках, реєстрах, звітах, архівах та інших видах інформаційних масивів і служить для належного забезпечення функціонування системи органів, що здійснюють контроль за додержанням податкового законодавства [130, с. 32].

Інформаційні ресурси органів ДФС України – це інформаційна інфраструктура та циркулююча в ній продукція інформаційної діяльності (збір, накопичення, аналіз, обробка), яка дає змогу розв'язувати відповідні завдання, що стоять перед органами ДФС України у процесі виконання своїх функцій, пов'язаних з ухиленням від сплати податків, зборів. Діяльність органів ДФС України має на меті отримання інформації, її накопичення, обробку, аналіз, а також вжиття відповідних заходів реагування на отриману інформацію [111, с. 225].

В інформаційних ресурсах, які функціонують в органах ДФС, містяться відомості, що відображають у податковій звітності та документах, які надаються під час проведення митних процедур, а також інших документах, в яких відображається податкова або митна інформація.

Крім того, інформаційні ресурси органів ДФС включають сукупність електронної інформації та відомостей, створених та накопичених в інформаційних та телекомунікаційних системах.

Основними інформаційними ресурсами органів ДФС, які використовують під час поточної діяльності співробітники, є такі:

– інформаційна система «Податковий блок», до складу якої входять такі підсистеми: «Обробка податкових зобов'язань та платежів», «Облік платежів», «Податковий аудит», «Реєстрація платника податків», «Аналітична система»;

– автоматизована інформаційна система «Архів електронної звітності», в якій збираються, зберігаються та опрацьовуються документи, які надходять від платників податків, зборів. Такими документами є: податкові накладні, податкові декларації, запити, відповіді ДФС тощо. У структурі зазначеної автоматизованої системи діє інформаційна система «Єдиний реєстр податкових накладних», в якій закріплена інформація про зареєстровані та виписані податкові накладні підприємців;

– автоматизована система митних оформлень «Інспектор», в якій відображено інформацію про проведені імпортні або експортні операції підприємствами й громадянами, оформлені митні декларації;

– інформаційна система «Галузь», в якій закріплено інформацію про розрахунки з бюджетом суб'єктами господарювання та громадянами;

– автоматизована інформаційна система «Управління документами», за допомогою якої опрацьовується вхідна та вихідна кореспонденція органів ДФС України на всіх рівнях управління.

Неналежна організація роботи з управління інформаційними ресурсами та захисту інформації, яка в них циркулює, може призвести до витоку такої інформації або її знищення. Зокрема, у грудні 2015 року через збій у роботі АІС «Управління документами» в ДФС України втрачено три терабайти інформації (близько 531 тис. електронних документів, 26 тис. даних реєстраційних карток, 4,1 тис. реєстраційних карток, 3,1 тис. контрольних карток). Причинами збою функціонування вказаної інформаційної системи стали: застарілість обладнання, неможливість забезпечити належні умови для

розташування сервірів, відсутність обслуговування системи зберігання даних та належного рівня захисту інформації.

Для унеможливлення пошкодження інформаційних ресурсів органів ДФС України та знищення інформації необхідно систематично здійснювати оновлення програмного забезпечення (криптографічних, технічних, інших заходів) із захисту податкової та митної інформації, підтримувати високий рівень інформаційного забезпечення підрозділів ДФС для того, щоб уникнути застарілості комп'ютерних засобів, обладнання та сервірів.

Належне функціонування інформаційних ресурсів в органах ДФС України обумовлює забезпечення надійного захисту податкової й митної інформації, ефективну взаємодію з платниками податків, а також мінімізацію суб'єктивного впливу на підприємців з боку фіскальних органів та їх службовців.

Створення державних інформаційних ресурсів у структурних підрозділах ДФС України виконується на підставі інформації, отриманої від громадян, органів державної влади, органів місцевого самоврядування, господарських організацій і громадських об'єднань. Звичайно інформаційні ресурси є власністю держави та перебувають у веденні органів державної влади й відповідних організацій, згідно з їх компетенцією, та підлягають обліку і захисту, який забезпечує держава. Органи державної влади України створюють державні інформаційні ресурси, які перебувають в їхньому веденні та забезпечують їхнє використання відповідно до встановлених цілей.

Отже, вважаємо доцільно запропонувати таке визначення управління інформаційними ресурсами органів ДФС України – це встановлена законодавством діяльність органів ДФС України щодо реалізації правових, організаційних, управлінських і технічних заходів, спрямована на належне отримання, накопичення, опрацювання, використання й зберігання інформації, необхідної для виконання покладених на ДФС функцій.

## 2.4. Адміністративна відповідальність у сфері забезпечення інформаційної безпеки ДФС України

Інформація як така завжди була важливим чинником у прийнятті рішень на всіх рівнях та етапах розвитку соціальної сфери та держави. Берг А.І. зазначив: «інформація проникає у всі пори життя людей і суспільства, а життя неможливе в інформаційному вакуумі». У зв'язку з тим, що суспільство перейшло на новий інформаційний рівень, з'явилася необхідність захистити інформацію усіма правовими та комплексними засобами. Одним з них є адміністративна відповідальність за інформаційні порушення.

Формулюючи поняття «адміністративне правопорушення», Кодекс України про адміністративні правопорушення від 24 грудня 1984 р., (далі – КупАП) визнав адміністративну караність діяння як його невід'ємну ознаку, тобто обов'язкове настання адміністративної відповідальності особи, яка вчинила адміністративне правопорушення.

Закон України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII у редакції від 13 січня 2011 р. у ч. 1 ст. 6 визнав установлену законодавством відповідальність за інформаційні правопорушення невід'ємною гарантією забезпечення права особи на інформацію [22], що може розглядатись як невідворотність настання покарання за ці правопорушення.

У межах інформаційної сфери адміністративна відповідальність, як ознака правопорушень, віддзеркалює правову реакцію держави за вчинене діяння (дію чи бездіяльність), покладає на правопорушника негативні наслідки застосування санкцій адміністративно-деліктних норм як результату вчиненого правопорушення [106, с. 123].

У галузі адміністративного права переважає думка, що адміністративна відповідальність – це реалізація тільки адміністративних стягнень [100, с. 45]. Ця позиція відображена і у ст. 23 КУпАП, яка передбачає, що

адміністративне стягнення є мірою відповідальності, яка застосовується з метою виховання особи, яка вчинила адміністративні правопорушення [8].

Проте необхідно зазначити, що сучасний КУпАП є відображенням командно-адміністративних методів державного регулювання стосовно всіх сфер людського життя. Ряд суспільних правопорушень та відповідальність за їхнє здійснення передбачені Кримінальним кодексом, але найбільший блок суспільних правопорушень законодавцями радянського періоду закріплено в Кодексі України «Про адміністративні правопорушення». Однак зауважимо, що адміністративне право розгдядається, як галузь права, що обслуговує управлінські відносини. Тобто можемо стверджувати, що всі правопорушення, які подано в КУпАП, можна розглядати, як правопорушення громадян проти адміністрації. Проте, можливо, їх потрібно розглядати навпаки, як правопорушення адміністрації проти громадян. Як наслідок, цілі блоки норм КУпАП на сьогодні не діють або постійно змінюються.

Відповідно до законодавства України існують різні форми та методи юридичної відповідальності за недотримання норм та їх порушення. Вони поділяються за різними властивостями та характером впливу.

Науковці, які вивчають проблемні питання адміністративних правопорушень у сфері забезпечення інформаційної безпеки органів ДФС України, вважають що, беручи до уваги немайнову природу інформації, її здатність до необмеженого тиражування, часту не пов’язаність з матеріальним носієм або безпосереднім власником, властивість до зміни як за змістом, так і за формою, найбільш поширеним видом відповідальності за адміністративні правопорушення у сфері забезпечення інформаційної безпеки ДФС України є майнові стягнення, насамперед штрафні [137, с. 9].

У положеннях щодо відповідальності, зокрема законах України «Про інформацію», «Про захист персональних даних», «Про телебачення і радіомовлення», «Про доступ до публічної інформації», відображені тільки диспозиції правопорушень. У зв’язку з тим, що в них не визначено санкції,

адміністративні норми виконуються здебільшого несумлінно. Тобто, нормативне закріплення адміністративної відповідальності у сфері забезпечення інформаційної безпеки органів ДФС України є важливим фактором захищності інформації та інформаційних ресурсів.

Підставою для виникнення адміністративної відповідальності за інформаційні правопорушення є здійснення суб'єктом (учасником) інформаційних правовідносин правопорушення у сфері інформаційної безпеки органів ДФС України. Крім того, потрібно визначати інформаційне правопорушення у діяльності ДФС України, як протиправну, винну (умисну або необережну) дію чи бездіяльність суб'єкта інформаційних відносин, який посягає на встановлений законодавством правопорядок у податковій чи митній сферах держави щодо обробки персональних даних, доступу до інформації, її захисту, а також посягає на функціонування інформаційних технологій та інформаційних ресурсів ДФС України, за яку законом передбачено юридичну відповідальність.

Посадові особи органів ДФС, громадяни та службові особи підприємств, які мають доступ до згаданої вище інформації, або відіграють певну роль у правовідносинах, є суб'єктами інформаційних правопорушень.

Об'єктами таких інформаційних правопорушень у різних сферах забезпечення інформаційної безпеки органів ДФС можуть виступати інформація, архіви ДФС України, інформаційні системи ДФС України, правила їх використання та збереження інформації в них, а також відносини щодо правового режиму поширення конфіденційної, таємної та службової інформації.

Адміністративна відповідальність за інформаційні правопорушення міститься у різних главах КУпАП та передбачена такими статтями 148-5, 163-5, 163-9, 163-11, 164, 164-3, 164-12, 164-14, 166-4, 166-9, 166-10, 184-2, 186-3, 188-5, 188-11, 188-14, 188-18, 188-32, 188-35, 188-36 тощо [8].

Розглядаючи актуальні питання та напрями вдосконалення інформаційної безпеки в органах ДФС, необхідно зауважити, що

адміністративне стягнення за інформаційне правопорушення у вигляді штрафу не зовсім відповідає реальній заподіяній шкоді.

Крім того, на законодавчому рівні розробляються нові нормативні акти щодо організаційних і правових засад у сфері забезпечення інформаційної безпеки органів ДФС України, враховуючи юридичну відповідальність. Як наслідок, необхідно узгоджувати такі розроблювані положення з уже існуючими шляхом внесення доповнень до останніх. Так, 09.05.2011 р. набув чинності Закон України «Про доступ до публічної інформації». Відповідно до статті 24, відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень: ненадання відповіді на запит; ненадання інформації на запит; безпідставна відмова у задоволенні запиту на інформацію; неоприлюднення інформації у порядку статті 15 Закону; надання або оприлюднення недостовірної, неточної або неповної інформації; несвоєчасне надання інформації; необґрунтоване віднесення інформації до інформації з обмеженим доступом; нездійснення реєстрації документів; навмисне приховування або знищення інформації чи документів [31]. Але відповідальність за всі діяння, визначені у Законі протиправними, у КУпАП не передбачена, однак певні зміни внесені.

Для виконання завдань із виявлення і протидії адміністративним правопорушенням у сфері забезпечення інформаційної безпеки органів ДФС України в науці адміністративно-деліктного права України позитивним визнано досвід зарубіжних країн щодо встановлення розміру адміністративних штрафів у мінімальних заробітних платах [153, с. 7].

Динамічна природа мінімальної заробітної плати як облікової фінансової одиниці сприяє наближенню розміру адміністративної відповідальності до наслідків протиправної поведінки, що забезпечить функціонально-правову єдність, узгодженість і невід’ємність законодавчо встановлених ознак адміністративних деліктів у сфері забезпечення інформаційної безпеки органів ДФС.

Враховуючи викладене, вважаємо обґрунтованою науково пропозицію щодо потреби замінити неоподаткованої мінімум доходів громадян на мінімальний розмір заробітної плати при встановленні адміністративної відповідальності у формі штрафу у зв'язку з модернізацією адміністративно-деліктного законодавства, розробки проекту Адміністративно-деліктного кодексу України.

Об'єднання на законодавчому рівні значної кількості адміністративних правопорушень у сфері забезпечення інформаційної безпеки ДФС України за ознакою виду адміністративної відповідальності та санкції не завжди тягне за собою настання для правопорушника однакових за кількісними критеріями наслідків протиправної поведінки.

Санкції окремих адміністративно-деліктних норм, зокрема ст. ст. 51-2, 53-2, 91-4, 145, 146, 148, 148-2, 148-3, 148-5, установлюють широкі мінімальні та максимальні межі негативного, примусового впливу на поведінку порушника одних і тих самих обмежень і заборон у сфері забезпечення інформаційної безпеки ДФС України, що на практиці породжує виникнення додаткових корупційних ризиків [8].

Отже, закон, крім основних обставин, які обтяжують чи пом'якшують адміністративну відповідальність, фактично не встановлює додаткових критеріїв визначення остаточного розміру відповідальності відповідно до його мінімальних і максимальних меж. Вказане фактично ставить завдання перед уповноваженим органом адміністративної юрисдикції з визначення однієї із властивостей адміністративного правопорушення щодо призначення відповідальності за його вчинення.

Тобто, з позицій правозастосування, введення в дію санкцій вказаних адміністративно-деліктних норм у деяких випадках призведе до різних наслідків, які матимуть неоднозначний вплив на інтереси правопорушника. Це може призвести до того, що в рамках окремих видів адміністративних правопорушень щодо забезпечення інформаційної безпеки органів ДФС України адміністративна відповідальність за ці проступки може значно

відрізнятися за якісними показниками в однакових категоріях справ, що викликає зниження профілактичної дії адміністративних стягнень.

Для того,щоб усунути вказані корупційні ризики, забезпечити пропорційність покарань суспільно шкідливим наслідкам адміністративних правопорушень, удосконалити профілактичні дії майнових адміністративних стягнень у сфері забезпечення інформаційної безпеки органів ДФС України пропонуємо в нормах КУпАП закріпити загальне правило, відповідно до якого мінімальна межа майнової адміністративної відповідальності не може бути меншою за половину від його максимальної межі за конкретний різновид адміністративного правопорушення.

Аналіз норм чинного в Україні законодавства стосовно виявлення сутності адміністративної відповідальності як адміністративні правопорушення у сфері забезпечення інформаційної безпеки ДФС України дає можливість виділити ряд проблем, пов'язаних із цією властивістю адміністративних деліктів.

По-перше, визначаючи те або інше діяння як адміністративне правопорушення у сфері забезпечення інформаційної безпеки ДФС України, законодавець у окремих випадках не встановлює міру адміністративної чи будь-якої іншої юридичної відповідальності за його вчинення.

Законодавством України встановлена протиправність окремих діянь, однак не передбачена така важлива його ознака, як адміністративна відповідальність. Це, відповідно до загальноприйнятих поглядів в теорії та практиці адміністративної деліктології, виключає можливість кваліфікації діяння як адміністративного правопорушення [55].

Незважаючи на обов'язковість адміністративної відповідальності за діяння, визнані адміністративними правопорушеннями, законодавство України передбачає окремі склади проступків, не наділених такою властивістю [103, с. 4].

Винятком із загального правила є правопорушення, вчинені особами, на яких поширюється дія дисциплінарних статутів. Зазначені суб'єкти, як

правило, несуть відповідальність за дисциплінарними статутами, а тому адміністративна відповідальність, як ознака скоєних ними правопорушень, відсутня, хоча від цього такі проступки не перестають бути адміністративними, а лише відбувається заміна одного різновиду юридичної відповідальності іншим [103, с. 4].

По-друге, досвід законотворчого процесу у сфері забезпечення інформаційної безпеки органів ДФС України часто припускає формулювання рівнозначних складів адміністративних правопорушень у різновидових за юридичною силою актах адміністративного законодавства. Однак тільки одне з визначених порушень дотримується санкцією адміністративно-правової норми.

Така система правового регулювання характерна, зокрема, для відносин, що складаються у сфері забезпечення доступу до публічної інформації, у сфері обігу та використання державної, комерційної таємниці органами ДФС України. Так, Закон України «Про державну таємницю» від 21 січня 1994 р. № 3855-VII у ст. 39 закріплює 17 складів правопорушень, пов'язаних із державною таємницею, і лише 8 було відображено в ст. 212-2 КУпАП і забезпечено заходами адміністративної відповідальності [24].

Іншим прикладом того самого порядку є норма, закріплена у ч. 1 ст. 24 Закону України «Про доступ до публічної інформації» від 13 січня 2011 р. №2939-VI, якою встановлено 9 складів правопорушень у сфері забезпечення доступу до публічної інформації, однак тільки 3 з них були перенесені в норми ст. 212-3 КУпАП [31].

За загальним правилом з таких видів правопорушень адміністративним повинно визнаватися те, склад якого визначений диспозицією адміністративно-деліктної норми, що забезпечується відповідною адміністративно-правовою санкцією [137].

На підставі зазначеного вище, пропонуємо з вимог та положень ч. 1 ст. 24 Закону України «Про доступ до публічної інформації» та ст. 39 Закону України «Про державну таємницю» визначені в них склади проступків

вилучити, а ті з них, що не одержали самостійного закріплення в нормах адміністративно-деліктного законодавства, відтворити в приписах КУпАП з відповідними заходами адміністративної відповідальності.

Деякі дослідники, розглядаючи проблему встановлення адміністративних стягнень у сфері забезпечення інформаційної безпеки ДФС України поза нормами КУпАП, формулюють погляд, відповідно до якого види адміністративних правопорушень та адміністративні стягнення за їх вчинення мають визначатися спеціальними нормами галузевих законів, якими регулюються окремі види правовідносин [126, с. 214].

В основі наведеного погляду перебуває правовий зв’язок між структурними елементами інформаційних правовідносин у сфері забезпечення інформаційної безпеки ДФС України та наслідками порушення чинних для суб’єктів таких правовідносин обмежень і заборон, що забезпечує більш тісний зв’язок між правовідносинами, у межах яких вчинено правопорушення, самим правопорушенням та відповідальністю за його скоєння [137].

Концентрація в структурі КУпАП абсолютної більшості матеріальних і процесуальних адміністративно-деліктних норм має наслідком зменшення кількості бланкетних норм, дія яких проникає у сферу забезпечення інформаційної безпеки ДФС України, зменшує ризик пошкодження родових особливостей інформаційних правопорушень – адміністративних, дисциплінарних, кримінальних та цивільно-правових, чим забезпечується більш правильна, послідовна побудова правового механізму запобігання розвитку адміністративної деліктності у сфері забезпечення інформаційної безпеки ДФС України.

Не виключаючи ймовірності виникнення ризиків порушення норм інформаційного законодавства у сфері забезпечення інформаційної безпеки ДФС України, правового режиму інформації, інформаційних ресурсів, законами України встановлені обставини, при виникненні яких діяння, що за своїми формальними характеристиками є протиправними, адміністративним

правопорушенням не вважається, тому не тягне за собою використання адміністративних стягнень.

Єдиною обставиною, що визначає стаття 18 Кодексу України «Про адміністративні правопорушення» та виключає протиправність дій, є крайня необхідність.

Відповідно до ст. 18 КУпАП, «Не є адміністративним правопорушенням дія, яка хоча і передбачена цим Кодексом або іншими законами, що встановлюють відповідальність за адміністративні правопорушення, але вчинена в стані крайньої необхідності, тобто для усунення небезпеки, яка загрожує державному або громадському порядку, власності, правам і свободам громадян, установленому порядку управління, якщо ця небезпека за таких обставин не могла бути усунута іншими засобами і якщо заподіяна шкода є менш значною, ніж відвернена шкода» [8].

Відповідно до норми, передбаченої у ч. 2 ст. 32 Конституції України від 28 червня 1996 р. № 254к/96ВР, «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [1].

Таке положення Конституції України набуло подальшого розвитку у спеціальних нормах певних законів України відносно певних видів інформації: банківської, комерційної, публічної, службової та іншої.

Відповідно до ч. 2 ст. 8 Закону України «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VII, суб'єкти владних повноважень – розпорядники публічної інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини [31].

За правилами, закріпленими у ч. 1 ст. 11 цього Закону, «Посадові та службові особи не підлягають юридичній відповідальності, незважаючи на порушення своїх обов'язків, за розголошення інформації про

правопорушення або відомостей, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю» [31].

Аналіз змісту зазначених норм дозволив виявити, що у сфері забезпечення інформаційної безпеки органів ДФС України крайня необхідність являє собою дії учасників інформаційних правовідносин у податковій та митній сферах, спрямованих на розкриття інформації, що має обмежений доступ, надання доступу до інформаційних ресурсів та систем, які вважаються адміністративними правопорушеннями з формальним чи матеріальним складом, але у разі більшого ризику у відверненні шкоди для національної безпеки та економіки, таке правопорушення може визначатися не важливим для розгляду через ризик виникнення небезпек та більшої шкоди.

Конституцією України й іншими законодавчими актами встановлено коло обставин, при настанні яких протиправність діяння в інформаційній сфері загалом виключається, зокрема у сфері забезпечення інформаційної безпеки органів ДФС України [1].

Беручи до уваги зазначений вище законодавчий підхід, адміністративна відповідальність як невід'ємна ознака та безпосередній наслідок адміністративних правопорушень у сфері забезпечення інформаційної безпеки органів ДФС України віддзеркалює правове оцінювання країною протиправного використання інформації, інформаційних ресурсів, інформаційно-комунікаційних систем, фактів порушення права на інформацію фізичних або юридичних осіб.

Враховуючи значне посилення впливу інформації, інформаційно-комунікаційних систем на суспільні та державно-політичні процеси, розширення обсягу обігу інформації, чинне адміністративно-деліктне законодавство України у сфері забезпечення інформаційної безпеки ДФС

України потребує послідовної, системної модернізації в частині розширення складів адміністративних інформаційних правопорушень, розширення і посилення стягнень, що підлягатимуть застосуванню за їх вчинення як відносно фізичних, так і юридичних осіб – суб'єктів інформаційних правовідносин.

Отже, адміністративна відповідальність за вчинені інформаційні правопорушення – це процедура застосування до особи, яка визнана винною у вчинені відповідних дій або бездіяльності та яка здійснила інформаційне правопорушення, конкретних заходів впливу відповідно до санкції порушеної правової норми, яка застосовується у встановленому випадку. Така норма є частиною системи інформаційного правопорядку, який формує правову основу інформаційного суспільства. Важливе значення інформації в сучасному швидко прогресуючому суспільстві зумовлює актуалізацію адміністративної відповідальності в інформаційній сфері.

## Висновки до розділу 2

У процесі дослідження було зроблено такі висновки:

1. Встановлено, що за допомогою належного інформаційного забезпечення можлива найкраща продуктивність діяльності в податковій та митній сферах держави. Ефективність полягає у тому, що інформаційне забезпечення дозволяє оперативно збирати та опрацьовувати усі види інформації для органів ДФС, а саме: аналітичної, довідкової, статистичної, науково-технічної, митної, податкової тощо.

2. Інформаційне забезпечення управління в органах ДФС України являє собою сукупність організаційних, правових та технічних заходів, що формують інформаційні зв'язки складових системи управління за допомогою упорядкування інформації, баз даних і знань.

3. Інформаційне забезпечення органів ДФС України здійснюється стосовно: організації електронного документообігу; накопичення та збереження податкової й митної інформації в інформаційних ресурсах, автоматизованих інформаційних системах; опрацювання податкової й митної інформації, зокрема звітності; формування електронної бази нормативних документів.

4. Інформаційні відносини в податковій та митній сферах держави визначено як однорідну групу суспільних відносин, що виникають під час здійснення інформаційної діяльності органами ДФС, а саме під час створення, збирання, зберігання, одержання, використання, поширення, охорони та захисту інформації, необхідної для виконання покладених на ці органи функцій та завдань.

5. Захист інформаційних відносин та інформації в діяльності органів ДФС України визначено як сукупність дій, спрямованих на виявлення і протидію небезпекам та загрозам, що виникають під час функціонування інформаційних ресурсів та технологій. Такі заходи, зокрема, включають у себе: протидію порушенню змісту та цілісності інформації, конфіденційності та небажаному розголошенню інформації, її перекручуванню, а також зниженню рівня доступності інформації.

6. Визначено, що основними реальними та потенційними потребами у захисті інформації, яка має обіг в органах ДФС України, є загроза розголошення такої інформації, що, згідно з законодавством, становить державну чи іншу таємницю, а також службової інформації, що є власністю органів ДФС та спрямована на гарантування її інтересів (зокрема конфіденційної інформації, що є власністю фізичних або юридичних осіб – платників податків, зборів).

7. Визначено комплексний підхід до захисту інформації в органах ДФС, як якісний та дієвий процес нейтралізації можливих загроз безпеці інформації, що стосується збору та адміністрування податків, зборів.

8. Систему захисту інформації та інформаційних відносин в органах ДФС визначено як взаємопов’язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Для її створення необхідні заходи захисту інформації, які мають сертифікат відповідності або експертний висновок з позитивним результатом у сфері технічного та/або криптографічного захисту інформації.

9. Запропоновано авторське розуміння поняття «управління інформаційними ресурсами органів ДФС України», як встановлену законодавством діяльність органів ДФС України щодо реалізації правових, організаційних, управлінських і технічних заходів, спрямовану на належне отримання, накопичення, опрацювання, використання й зберігання інформації, необхідної для виконання покладених на ДФС функцій.

10. Встановлено, що створення державних інформаційних ресурсів в органах ДФС України здійснюється на підставі інформації, отриманої від громадян, органів державної влади, органів місцевого самоврядування, суб’єктів господарюванняі громадських об’єднань.

11. Інформаційні ресурси органів ДФС України є власністю держави, що перебувають у веденні ДФС України згідно з їх компетенцією та підлягають обліку і захисту, який забезпечується державою.

8. З’ясовано, що в інформаційних ресурсах, що функціонують в органах ДФС, містяться відомості, що відображаються у податковій звітності та документах, які надаються під час проведення митних процедур, а також інших документах, де відображається податкова або митна інформація. Інформаційні ресурси органів ДФС включають сукупність електронної інформації та відомостей, створених та накопичених в інформаційних та телекомунікаційних системах.

9. З’ясовано, що нормативне закріплення адміністративної відповідальності у сфері забезпечення інформаційної безпеки органів ДФС України є важливим фактором захищеності інформації та інформаційних ресурсів.

10. Підставою для виникнення адміністративної відповідальності за інформаційні правопорушення є здійснення суб'єктом (учасником) інформаційних відносин порушення законодавства у сфері інформаційної безпеки органів ДФС України.

11. Встановлено, що адміністративна відповідальність є невід'ємною ознакою та безпосереднім наслідком інформаційних правопорушень у діяльності органів ДФС України, що віддзеркалює правове оцінювання країною протиправного використання інформації, інформаційних ресурсів, інформаційно-комунікаційних систем, фактів порушення права на інформацію фізичних або юридичних осіб.

12. Зазначено, що адміністративне стягнення за інформаційне правопорушення в ДФС України у вигляді штрафу не завжди відповідає реальній заподіяній шкоді. Законодавством, крім основних обставин, які обтяжують чи пом'якшують адміністративну відповідальність, фактично не встановлено додаткових критеріїв визначення остаточного розміру стягнення відповідно до його мінімальних і максимальних меж. Вказане фактично ставить перед уповноваженим органом адміністративної юрисдикції завдання визначити одну із властивостей адміністративного правопорушення щодо призначення відповідальності за його вчинення. Це може призвести до того, що в рамках окремих видів адміністративних правопорушень щодо забезпечення інформаційної безпеки органів ДФС України адміністративна відповідальність за ці правопорушення може значно відрізнятися за якісними показниками в однакових категоріях справ, що викликає зниження профілактичної дії адміністративних стягнень.

# РОЗДІЛ 3

# НАПРЯМИ УДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

## 3.1. Актуальні питання удосконалення нормативно-правового регулювання інформаційної безпеки органів ДФС України

Розвиток системи нормативно-правового регулювання відносин у сфері інформаційного забезпечення є пріоритетним напрямом щодо організації інформаційної безпеки України та безпеки її національних інтересів. Ці чинники відіграють важливу роль у протидії загрозам таких інтересів та впорядкування відповідного правотворчого процесу.

Правове регулювання інформаційної безпеки органів ДФС України передбачає сукупність правових норм, які врегульовують відносини в цій сфері, та відповідні правозастосовні акти.

Правові норми складають основу інформаційної безпеки органів ДФС України й забезпечують належне законодавче функціонування діяльності органів ДФС України в інформаційній галузі. До цієї бази включаються і норми міжнародних договорів України, закони України, акти Президента України, постанови Кабінету Міністрів України, акти органів державної влади, які регулюють відносини у цій сфері. Однак певного перетворення потребує правова система України та законодавство у зв’язку з існуючими недоліками. Це підтверджує гостра потреба у правовому забезпеченні напряму на демократичні перетворення в суспільстві і державі.

Перед нашою державою постала необхідність прийняти ряд законодавчих актів, що мають відповідати європейським стандартам. Як зазначає Максименко Ю.Є. у своїй дисертації, аналіз стану нормативно-

правового регулювання інформаційної безпеки України здійснюється за трьома факторами:

1. Інформаційна безпека у сфері прав і свобод людини та громадянина.
2. Інформаційно-психологічна безпека.
3. Інформаційно-технічна безпека [105, с. 17].

Бондаренко С.В. під нормативно-правовим регулюванням інформаційної безпеки органів державної влади, зокрема ДФС, визначає форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою для їх упорядкування, закріплення і забезпечення [86, с.142].

На сьогодні одним із важливих напрямів стратегії адміністративно-правового забезпечення інформаційної безпеки органів ДФС України є аналіз і забезпечення належного рівня нормативно-правового регулювання в цій сфері.

Крім того, рівень інформаційного забезпечення та інформатизації цілком залежить від належного нормативно-правового врегулювання інформаційної безпеки в органах Державної фіскальної служби, що суттєво впливає на порядок адміністрування податків, зборів та обов'язкових платежів, взаємозв'язків з громадськістю, а також здійснює свій вплив на заходи, спрямовані на протидію економічним злочинам, ухиленню від сплати податків, зборів й обов'язкових платежів.

Так, пріоритетні напрями та головні принципи державної інформаційної політики закріплені в Національній програмі інформатизації в лютому 1998 р. [32], Концепції Національної програми інформатизації [44] й інших нормативних актах. Правовий фундамент інформаційних правовідносин в Україні становлять: Конституція України, закони України: «Про інформацію» [22], «Про захист інформації в інформаційно-телекомунікаційних системах» [13], «Про державну таємницю» [24], «Про захист персональних даних» [29], «Про телекомунікації» [28], «Про науково-технічну інформацію» [23], «Про інформаційні агентства» [25], «Про основні

засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [10] й інші нормативно-правові акти. Існуюча система законів у галузі інформатизації, обігу інформації, її захисту, у сфері зв'язку, телекомунікації дає можливість стверджувати про активне формування бази інформаційного законодавства в державі.

Законодавчу основу врегулювання інформаційних правовідносин у фіскальних органах становлять такі нормативно-правові акти:

– Конституція України від 28.06.1996, яка встановлює засади інформаційної функції держави та забезпечує інформаційні права, свободи людини, гарантії їх здійснення та обмеження (зокрема, право кожної особистості на інформацію – ст. 34, право особи давати згоду на збирання, зберігання, використання та поширення конфіденційної інформації про неї – ст. 32, право кожного на забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції – ст. 31, право людини на вільний доступ і поширення інформації про стан навколишнього середовища, про якість харчових продуктів і предметів побуту – ст. 50 тощо). У Конституції України у ч. 1 ст. 17 визначено забезпечення інформаційної безпеки однією з найважливіших функцій держави [1];

– Податковий кодекс України від 02.12.2010, положеннями якого регулюється порядок надання контролюючими органами платникам податків консультацій з питань практичного застосування окремих норм податкового законодавства (статті 52–53 ПК України), інформаційно-аналітичного забезпечення діяльності контролюючих органів (статті 71–74 ПК України), а також передбачено право платників податків на отримання інформації про податки і збори (стаття 17 ПК України) [5];

– Митний кодекс України від 13.03.2012, положеннями якого врегульовано питання реалізації органами ДФС державної митної справи (статті 5-8 МК України). Зокрема, встановлено порядок щодо дотримання вимог конфіденційності інформації (стаття 11 МК України), забезпечення інформування органами ДФС про прийняті рішення з питань державної

митної справи (статті 19-23 МК України); застосування інформаційних ресурсів та технологій в державній митній справі (статті 31-35 МК України) тощо [3];

– Кримінальний процесуальний Кодекс від 13.04.2012, положення якого регулюють порядок збирання, отримання та доступу до інформації, яка має значення для встановлення обставин кримінального правопорушення [9];

– Закон України «Про інформацію» від 02.10.1992, який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. У статті 5 цього Закону закріплено право кожного на інформацію, а статтями 10 і 16 передбачено такий вид інформації, як податкова інформація, правовий режим якої визначається Податковим кодексом України та іншими законами [22];

– Законом України «Про доступ до публічної інформації» від 13.01.2011 визначено порядок забезпечення права кожної особистості на доступ до інформації, яка перебуває у володінні суб'єктів владних повноважень й інших розпорядників публічної інформації, серед яких, згідно з положенням п. 1 ч. 1 ст. 13 вказаного закону, органи ДФС України [31];

– Закон України «Про захист персональних даних» від 01.06.2010, який регулює суспільні відносини щодо захисту персональних даних під час їх обробки. Органи ДФС України під час здійснення обліку платників податків, зборів обробляють персональні їхні дані, а тому є володільцями та/або розпорядниками баз персональних даних [29];

– Закон України «Про оперативно-розшукову діяльність» від 18.02.1992, який врегульовує порядок отримання, збирання та розпорядження інформацією, що становить оперативний інтерес (зокрема в статті 7 передбачені обов'язки підрозділів, які здійснюють оперативно-розшукову діяльність, а в статті 8 закріплені права цих підрозділів) [20];

– Закон України «Про державну таємницю» від 21.01.1994, який врегульовує порядок віднесення інформації до державної таємниці, також

порядок засекречування, розсекречування її матеріальних носіїв, охорону інформації, що становить державну таємницю [24];

– Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 врегульовує суспільні відносини, які виникають під час електронного документообігу. Також цей Закон встановлює організаційно-правові засади та порядок використання електронних документів. Так, платники податків, зборів та обов'язкових платежів здійснюють подання електронної податкової звітності до органів ДФС, що значно зменшує навантаження й забезпечує захист податкової і митної інформації [11];

– Закон України «Про електронний цифровий підпис» від 22.05.2003, в якому визначено нормативно-правовий режим електронного цифрового підпису та врегульовано суспільні відносини, що мають місце при використанні електронного цифрового підпису [27];

– інші законодавчі акти.

Правова база інформаційних відносин у податковій й митній сфері не обмежується названими законодавчими актами і доповнюється підзаконними нормативно-правовими актами. Так, на виконання положень ПК України щодо порядку отримання й використання інформації органами ДФС, Кабінетом Міністрів України в постанові від 27 грудня 2010 року № 1245 затверджено Порядок періодичного подання інформації органам ДФС та отримання ними інформації за письмовим запитом [38].

Також органами ДФС України винесено ряд відповідних наказів: наказ ДПА України від 08.06.2011 р. № 345 «Про затвердження форми запиту на інформацію, Інструкції щодо процедури подання запиту на інформацію, її отримання в ДПА України та Порядку складення та подання запитів на інформацію ДПА України» [52], наказом ДПА України від 14.01.2010 р. № 17 «Про затвердження Інструкції щодо порядку збору, обробки та надання оперативної інформації підрозділами оперативного реагування» [49] та інші підзаконні нормативно-правові акти.

Основні засади, напрями та пріоритети розвитку інформаційного суспільства в Україні визначені Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». Запровадження новітніх інформаційно-телекомунікаційних технологій в усі сфери суспільного життя, а також у діяльність державних органів, органів місцевого самоврядування, розвиток інформаційного суспільства є одними з пріоритетних напрямів державної політики. Для цього визначено цілий ряд завдань, що виникають перед правовою системою держави. У Законі зазначено, що для ефективного розвитку й функціонування інформаційного суспільства потрібно удосконалити систему законодавства, привести у відповідність з нормами міжнародного права з приводу інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства [10].

Сьогодні, як констатує Бєляков К.І., в Україні існує два шляхи щодо визначення нормативно-правового регулювання інформаційних правовідносин: перший підхід засновується на доктрині англо-американської (англосаксонської) системи права, що передбачає фрагментарне та часткове вирішення питань регулювання інформаційних правовідносин на законодавчому рівні; другий підхід – на доктрині європейської (континентальної) системи права, що передбачає легальне визнання галузей законодавства та їх систематизації на рівні кодифікації [63, с. 279].

На нашу думку, перший підхід не відповідає повною мірою специфіці правової системи України, оскільки правова основа держави зорієнтована та формується здебільшого на принципах континентальної системи права й характеризується відповідною швидкою реакцією на необхідність правового регулювання інноваційних відносин, у тому числі у суспільстві.

Під сучасним інформаційним законодавством науковці розуміють комплекс законів, міжнародних договорів і нормативних актів, що регламентують правовідносини в галузі збирання, опрацювання, збереження і використання інформації. Недоліками законодавства, на думку

Стоєцького О. В., є такі: частина положень застаріла, недостатньо розроблені юридичні механізми реалізації і захисту права на інформацію, наявна термінологічна невпорядкованість, мають місце суперечності в регулюванні певних суспільних відносин різними законами, що призводить до неоднозначного тлумачення їх норм та створює труднощі для їх застосування [146, с. 9].

У разі коли чітко розглянути загальну масу вказаних правових актів, то можна виокремити основні групи за напрямами їхнього впливу та основні тенденції відносно нормативно-правового регулювання суспільних відносин.

По-перше, основу становлять законодавчі акти, що визначають стратегію розвитку загальних тенденцій формування інформаційних відносин, інформатизації, інформаційного суспільства, наприклад, закони України «Про національну програму інформатизації» [32], «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [10], «Про інформацію» [22].

По-друге, це цілий ряд нормативних документів, спрямованих на реалізацію основних завдань, поставлених у стратегічних законодавчих актах, наприклад, Розпорядження КМ України «Про затвердження плану заходів з виконання завдань, передбачених Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [10].

По-третє, це нормативно-правові акти адміністративного впливу та індивідуальної дії. Наприклад, постанова КМУ «Про керівника Національної програми інформатизації».

Стоєцький О.В. вважає, що реформування інформаційного законодавства необхідно здійснювати в декілька етапів: 1) прийняття нової редакції Закону України «Про інформацію» й внесення певних змін до інших нормативно-правових у цій галузі; 2) систематизація інформаційного законодавства, що передбачає консолідацію, інкорпорацію та кодифікацію; 3) розробка та прийняття Інформаційного кодексу України [146, с. 11].

У зв’язку із швидким розвитком інформаційних технологій у законодавстві України набули поширення нормативно-правові акти, створені, щоб регулювати дотримання положень інформаційної безпеки, а також прав та сводоб людини і громадянина. Як наслідок, необхідно оперативно реагувати на зміни, що відбуваються у цій сфері.

Особливим недоліком правового врегулювання інформаційної безпеки органів ДФС України є розпорошення цього питання у багатьох нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами.

Не менш важливою проблемою для високого рівня забезпечення інформаційної безпеки органів ДФС України є неузгодженість законодавчих та підзаконних нормативних актів як між собою, так і з чинною Конституцією.

Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації правових норм, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки. Крім того, наявність численних бланкетних чи відсильних правових норм, багатьох абстрактних і суб’єктивних понять, які потребують офіційного тлумачення чи чіткого визначення, а також відсутність закріплення фундаментальних, базових дефініцій (наприклад, інформаційна безпека) є джерелами загроз інформаційній безпеці України загалом та органам ДФС України зокрема [105, с. 12].

Ліпкан В.А. зазначає, що інформаційна безпека України є необхідною складовою національної безпеки. Важливим аспектом формування базових знань й уявлень про національну безпеку є розгляд та аналіз інформаційної безпеки. Стабільне функціонування суспільства й держави зумовлене рівнем розвитку, якістю функціонування та безпекою інформаційного середовища, а також рівнем і станом нормативно-правового регулювання вказаних процесів. Інформаційне законодавство закріплює положення й вимоги

державної інформаційної політики, що передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, розвиток інформаційних технологій та засобів захисту інформації, захист авторських і суміжних прав тощо [101, с. 194].

На сьогодні питання забезпечення національних інтересів і національної безпеки в інформаційній сфері перебуває на етапі розвитку. Забезпечення інформаційної безпеки вілбувається завдяки провадженню однієї цілісної державної політики національної безпеки у всіх сферах, у тому числі в інформаційній, включає у себе комплекс заходів економічного, політичного й організаційного напрямів, спрямованих на подолання небезпек і загроз інтересам людей, соціума та держави в цій сфері.

Для забезпечення та підтримання потрібного рівня безпеки в інформаційній сфері країни запроваджено комплекс юридичних норм, що управляють відносинами у цій сфері та розроблено головні напрями діяльності органів державного управління. Нині відбувається формування або перетворення органів забезпечення інформаційної безпеки і механізмів нагляду й контролю за їх діяльністю.

На нашу думку, доцільним є висловлювання Ліпкана В.А., що система забезпечення інформаційної безпеки в органах ДФС України не обмежується лише великим масивом нормативно-правових актів. Констатувати остаточне створення основних елементів системи забезпечення інформаційної безпеки в органах ДФС України не можна. Це зумовлено несформованістю загальної системи забезпечення національної безпеки, невизначеністю політики національної безпеки, а тому й визначає несформованість і інформаційної безпеки. Врешті-решт, недосконалість правового регулювання національної й інформаційної безпеки негативно впливає на державне управління в цілому у зазначеній сфері [101, с. 220 - 221].

Для покращення ситуації необхідно суттєво змінювати заходи щодо безпеки, упроваджувати дієві підходи до забезпечення інформаційної безпеки, без яких не відбуватиметься захист і розвиток інформаційної

системи в органах ДФС України. Моделювання загроз, які можуть виникати в інформаційній сфері органів ДФС України, а також розробку заходів і засобів захисту здійснюють окремі державні органи та підрозділи ДФС.

Тільки у межах функціонального підходу можливо в інтересах інформаційної безпеки органів ДФС задіяти існуючий інтелектуальний, організаційний, матеріально-технічний потенціал, забезпечити взаємодію міністерств і відомств, координацію їх діяльності. Основним є те, що функціональний підхід дозволяє оцінювати і прогнозувати стан системи управління та ефективність управлінських дій щодо попередження або нейтралізації загроз інформаційній безпеці органів ДФС України.

Необхідність зміни погляду щодо інформаційної безпеки органів ДФС України випливає також із норм Основного Закону України, зокрема статті 17, відповідно до якої інформаційна безпека віднесена до найважливішої функції держави та справи всього українського народу.

Безпека інформаційних ресурсів органів ДФС України на етапах впровадження міжнародної взаємодії визначається як елемент усієї системи захисту інформації та важлива складова інформаційної безпеки.

Загальну концепцію інформаційної безпеки органів ДФС України коротко можна визначити як систему запропонованих дій, що впливають на забезпечення права на інформацію і свободи інформаційної діяльності, на захист інформації і права власності на інформацію, на захист від інформації та від інформаційних впливів. Основою для удосконалення системи забезпечення інформаційної безпеки органів ДФС України у процесі розширення міждержавного співробітництва має бути ефективно діюча загальна система забезпечення інформаційної безпеки органів ДФС України як важлива складова національної безпеки України.

Інформація, сфера інформаційних технологій визначається як комплекс елементів усіх сфер життя і роботи суспільства та його системи, а інформаційна безпека – найважливіший і найвпливовіший фактор, що впливає на стан усіх адміністративних одиниць і сфер та інших складових

національної безпеки. Необхідно зазначити, що вимоги інформаційної безпеки органів ДФС України повинні органічно включатися у всі рівні законодавства, в тому числі і в конституційне законодавство, основні загальні закони, закони щодо організації державної системи управління, спеціальні закони, відомчі правові акти тощо. Розглянемо більш детально структуру правових актів, орієнтованих на забезпечення інформаційної безпеки органів ДФС України.

До першого блоку належить конституційне законодавство. Правила, які застосовують щодо питань інформатизації, інформаційного забезпечення органів ДФС України розуміються як складові елементи.

Другий блок – загальні закони, кодекси, що передбачають норми з питань інформаційної безпеки органів ДФС України.

Третій блок – закони про управління та його організацію, які стосуються окремих підрозділів органів ДФС України й визначають їхній статус. Зазначені закони передбачають норми щодо забезпечення інформаційної безпеки органів ДФС України. Разом із питаннями інформаційного забезпечення та інформаційної безпеки органів ДФС України, ці норми мають встановлювати й обов'язки з формування, актуалізації інформаційної безпеки органів ДФС України, адже це становить державний інтерес.

До третього блоку нормативно-правового регулювання інформаційної безпеки органів ДФС України можна віднести:

– загальнодержавні, міжвідомчі напрями національної політики інформаційної безпеки органів ДФС України, які реалізуються органами ДФС України у сферах її відання;

– дотримання захисту прав і законних інтересів людини, суспільства, держави;

– гарантування інформаційного суверенітету;

– реалізація й формування національної інформаційної політики й збільшення її ролі під час виконання інформаційної політики в органах ДФС України;

– забезпечення безпечності функціонування всіх складових інформаційного середовища ДФС України і його інтегрування у державний інформаційний простір;

– створення цілісної системи охорони та технічного захисту інформації, що має обмежений доступ, яка підлягає охороні з боку держави;

– забезпечення безпеки інформаційно-телекомунікаційних систем, мереж зв'язку та використання Інтернету;

– захист національних інтересів у процесі міжнародного співробітництва;

– прогнозування ризиків державної внутрішньої і зовнішньої політики, соціально-економічного розвитку, державного будівництва; потенційних і реальних інформаційних загроз, викликів і небезпек;

– адекватне реагування на негативні інформаційні чинники, виявлення, попередження і нейтралізація джерел внутрішніх і зовнішніх інформаційних загроз ДФС України;

– участь у двосторонніх і багатосторонніх системах забезпечення міжнародної інформаційної безпеки ДФС України;

– забезпечення загальнодержавного керівництва, координації і контролю у сфері реалізації державної політики з питань інформаційної безпеки органів ДФС України та оцінки її результативності.

Четвертий блок включає спеціально розроблені закони, які регламентують податкові й митні правовідносини. Саме зміст цього блоку законів і створює основу правового регулювання інформаційної безпеки органів ДФС України.

До п'ятого блоку входять підзаконні нормативно-правові акти щодо дотримання інформаційної безпеки органів ДФС України.

Шостий блок передбачає законодавство нашої держави, яке містить у собі норми про юридичну відповідальність за вчинені правопорушення у

сфері дотримання інформаційної безпеки органів ДФС України [163, с. 36 – 37]

На нашу думку, підгрунття правового регулювання інформаційної безпеки органів ДФС України повинні складати Конституція України, Концепція інформаційної безпеки України, закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, також підзаконні нормативно-правові акти, видані на їх виконання. Необхідно зазначити, що дана ця суспільних відносин регулюється більше ніж 30 законами.

Спеціальне законодавство у галузі безпеки інформаційної діяльності (інформаційної безпеки) ДФС України представлено сукупністю законів. Серед них важливе місце належить Закону Україіни «Про інформацію», який є базовим та закладає основу правового обгрунтування всіх найважливіших складових інформаційної діяльності органів ДФС України, зокрема:

– у ньому закріплено права громадянина та людини на інформацію, закладений правовий фундамент інформаційної діяльності;

– спеціальні закони України «Про інформацію», «Про інформаційну безпеку», Концепція інформаційної безпеки України, закони, які забезпечують інформаційну безпеку в податковій й митній сферах;

– підзаконні нормативні акти, які визначають й обгрунтовують правовідносини щодо забезпечення інформаційної безпеки органів ДФС України, а також щодо взаємодії з іншими державними органами тощо;

– створення системи наукового, матеріально-технічного, фінансового і кадрового забезпечення з метою дотримання інформаційної безпеки органів ДФС України;

– контроль і нагляд за реалізацією чинного законодавства щодо гарантування інформаційної безпеки органів ДФС України;

– застосування адміністративної, цивільно-правової та кримінальної відповідальності за вчинені порушення законодавства про інформаційну безпеку.

Необхідно зазначити, що Законом України «Про основи національної безпеки України» передбачено дев'ять сфер національної безпеки: зовнішньополітичну, державну безпеку, економічну, соціальну та гуманітарну, воєнну та сферу безпеки державного кордону України, внутрішньополітичну, екологічну, науково-технологічну та інформаційну. Отже, інформаційна безпека є складовою національної безпеки. У законі системно сформульовані основні функції, які має виконувати система забезпечення національної безпеки в усіх зазначених сферах. Конкретизація їх (з урахуванням особливостей інформаційної сфери) дає можливість визначити основні функції системи забезпечення інформаційної безпеки України. Але при загальному зростанні кількості законів, що приймаються, поки що залишається багато таких сфер життя суспільства і громадян, які донині не врегульовані на законодавчому рівні, що дає простір відомчій правотворчості. Національний банк, ДФС України, Фонд держмайна, інші центральні та місцеві органи виконавчої влади буквально «наплоджують» нормативні правові акти, до яких самі з не меншою швидкістю вносять зміни та доповнення [33].

Недостатнє врегулювання нормативно-правової бази стосовно інформаційних правовідносин певною мірою ускладнює реалізацію якісних змін у цій сфері. На сьогодні, враховуючи недостатність взаємопов'язаних й чітких заходів і теоретичних розробок із забезпечення інформаційної безпеки ДФС України, виникає ряд перешкод під час реалізації державними органами інформаційної безпеки, яка є невід'ємною частиною національної безпеки. Тільки реалізація науково обґрунтованої національної інформаційної політики може створити ефективну систему виявлення правопорушень у цій сфері.

Для гарантування інформаційної безпеки органів ДФС України пропонуємо встановити інститут податкової й митної таємниці. Під податковою таємницею потрібно розуміти сукупність інформації з обмеженим доступом для широкого кола осіб, яка містить персональні дані

фізичних та юридичних осіб, конфіденційну і службову інформацію, а також державну таємницю, та яка стає відомою органам ДФС у зв'язку з виконанням покладених на них функцій і підлягає захисту.

Митну таємницю будемо роглядати як сукупність інформації, що стає відомою органам ДФС під час реалізації державної митної справи та містить персональні дані фізичних та юридичних осіб, конфіденційну, службову інформацію, державну таємницю, використовується органами ДФС тільки для виконання митних завдань і підлягає захисту. Така інформація не може піддаватися розголошенню без дозволу суб'єкта, осіб чи органу, який надав указану інформацію. Крім того, митна таємниця включає в себе інформацію щодо підприємств, громадян, товарів, транспортних засобів, яку збирають, використовують органи ДФС, вносять до інформаційних систем.

У ст. 11 МК України викладено вимоги щодо дотримання конфіденційності інформації. Зокрема, у ч. 1 та ч. 2 вказаної статті наведено перелік митної інформації, яка не може розголошуватись і використовується з обмеженнями, передбаченими для інформації з обмеженим доступом.

Пропонуємо такі основні напрями правового регулювання інституту податкової й митної таємниці:

– виділення двох видів податкової й митної інформації: інформація з обмеженим доступом та відкрита інформація;

– поширення режиму таємниці лише на податкову й митну інформацію з обмеженим доступом;

– закріплення у ПК України систематизованого переліку податкової інформації, яка є інформацією з обмеженим доступом.

У зв'зку з цим вважаємо доцільно внести зміни до статті 72 ПК України, в якій закріплено порядок збору податкової інформації. Необхідно додати до вказаної статті пункт 72.2, в якому викласти перелік податкової інформації, яка є службовою інформацією та закріпити вимоги щодо її конфіденційності. Зокрема, пропонуємо пункт 72.2 статті 72 ПК України викласти в такій редакції:

«72.2.1. Службовою інформацією в органах ДФС є така: податкова інформація та інформація з питань податкових перевірок; з питань дотримання охорони державної таємниці, технічного та криптографічного захисту інформації; відомості стосовно інформатизації; інформація, що стосується роботи з особовим кадровим складом; інформація, отримана під час здійснення правоохоронної діяльності; відомості стосовно мобілізаційної роботи та цивільного захисту; інформація, яка опрацьовується не секретним діловодством; митна інформація.

72.2.2. За несанкціоноване розголошення відомостей, які містять службову інформацію, посадові особи органів ДФС несуть відповідальність, передбачену чинним законодавством.

72.2.3. Відомості, які містять у собі службову інформацію, надаються розпорядником інформації, якщо він правомірно раніше її оприлюднив.

72.2.4. Службова інформація має надаватися розпорядником інформації, якщо відсутні законні підстави для обмеження у доступі до вказаної інформації, що були раніше.

72.2.5. Конфіденційна інформація, яку збирають, використовують і формують органи ДФС, розголошується з дозволу фізичної або юридичної особи, які є власниками такої інформації.

Конфіденційна інформація може поширюватися тільки за згодою осіб, які обмежили доступ до такої інформації, а у разі відсутності згоди – тільки в інтересах національної безпеки, економічного добробуту та прав людини».

Ми погоджуємося з Бабіним І.І., який зазначає, що інститут податкової таємниці є комплексним правовим інститутом, що містить норми податкового, інформаційного, адміністративного, кримінального й інших галузей права, однак саме в Податковому кодексі України доцільно визначити чіткий перелік податкової інформації, яка є інформацією з обмеженим доступом і на яку поширюється режим податкової таємниці [59, с. 100].

Дослідження національного законодавства України, у якому встановлено правила безпеки, охорони та захисту інформації, становить собою комплекс збереження податкової й митної таємниці. Законом установлено поширення такої системи захисту на інформацію, яка становить державну, службову, комерційну, банківську, нотаріальну, аудиторську, адвокатську, таємницю страхування та інші визначені законодавством України таємниці.

Разом з тим, на сьогодні органи ДФС України мають як фіскальну, сервісну, так і правоохоронну функцію. З урахуванням цього набуває суттєвого значення для ефективного забезпечення інформаційної безпеки дослідження правових засад інформаційного гарантування виявлення, протидії та розслідування злочинів підрозділами податкової міліції. Зазначені питання пов’язані із необхідністю системного аналізу як правових засад щодо регулювання, створення та функціонування інформаційних систем і криміналістичних обліків в органах ДФС України, так і аналізом законодавчих норм, у тому числі уведених Податковим кодексом та Кримінальнім процесуальним кодексом [133, с. 177].

Отже, враховуючи велику кількість повноважень, які виконують органи ДФС України у сфері забезпечення інформаційної безпеки, забезпечення податкової й митної таємниці, все-таки спостерігається неврегульованість певних відносин у цих сферах. Вважаємо, вирішенню питань цієї сфери можуть сприяти:

1. Виділення основоположних функцій щодо забезпечення й дотримання інформаційної безпеки до повноважень органів ДФС України.
2. Розробка інститутів податкової й митної таємниці.
3. Виокремлення та закріплення в Податковому кодексі України переліку податкової інформації, яка вважається інформацією з обмеженим доступом та входить до режиму податкової таємниці.

Постала гостра потреба в розробленні єдиного комплексного системоутворюючого законодавчого акта, який зміг би забезпечити:

– створення єдиної стратегії формування державної політики щодо інформаційної безпеки органів ДФС України;

– розроблення правових та організаційних механізмів дотримання інформаційної безпеки органів ДФС України;

– виділення нормативно-правового статусу учасників інформаційних правовідносин органів ДФС України, встановлення їх відповідальності за дотримання законодавства у цій сфері;

– підготовка кадрів, які мають забезпечувати інформаційну безпеку органів ДФС України [115, с. 46].

Головними шляхами функціонування та дотримання правового режиму інформації в органах ДФС України є: забезпечення юридичних та технічних можливостей щодо доступу, обробки, збереження та передавання інформації; гарантування захисту інформації в органах ДФС України; доступ до автоматизованих інформаційних систем органів ДФС України з дотриманням відповідних механізмів захисту інформації, яка до них вноситься; впровадження в діяльність органів ДФС новітніх інформаційних систем та технологій, а також вдосконалення їхнього захисту; прийняття оновлених державних програм, спрямованих на вдосконалення правового забезпечення обігу податкової й митної інформації в державі, враховуючи міжнародний досвід та положення європейського законодавства; збільшення інформаційного обміну між національними органами та зарубіжними податковими й митними органами, що зумовлено транснаціональністю інформаційних правопорушень.

Підсумовуючи, можемо стверджувати, що на сьогодні в нашій державі сформувалася досить велика та об’ємна правова база. Питання, що виникають відносно створення, впровадження та використання інформаційних систем для реалізації головних завдань у певній галузі або державній установі розглядаються на рівні законів, указів Президента, постанов Кабінету Міністрів, які містять норми, правові приписи, указівки на права чи обов’язки органів державної влади використовувати інформаційні

системи для сприяння виконанню завдань та функцій, покладених на ці органи.

### 3.2. Міжнародний досвід реалізації адміністративно-правових засобів забезпечення інформаційної безпеки та шляхи його використання в Україні

Людина має безліч прав, але право на інформацію є одним з головних та слугує інструментом для реалізації нею інших прав та свобод. Отримання інформації про діяльність органів державної влади і місцевого самоврядування також входить до цього права та надає людині широкі можливості. Однак сутність права на інформацію має досить вільну інтерпретацію термінологічними засобами у національному законодавстві і інколи набуває не зовсім чіткого визначення порівнянно з міжнародно-правовими стандартами розуміння справедливості, свободи і верховенства права.

Так, ст. 19 Загальної декларації прав людини, прийнятої 10 грудня 1948 року Генеральною Асамблеєю ООН, надано право кожному шукати, отримувати, поширювати інформацію у будь-який вільно обраний спосіб і незалежно від кордонів [2].

Конституцією України кожній особистості гарантується право на свободу слова і думки, на вільне вираження своїх поглядів і переконань. Кожна людина має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в будь-який інший спосіб – на свій вибір. Реалізація вказаних прав може обмежуватися законом в інтересах національної безпеки, територіальної цілісності або громадського порядку для запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню

інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (ст. 34 Конституції України) [1].

На думку Письменицького А.А., в такій інтерпретації не тільки здійснюється заміна: «пошуку» на «збирання», що не є тотожними поняттями, але й обмеження обсягу самого права з виключенням з його структури положення про незалежність «від кордонів». Крім того, «розмивається» по інших нормативних актах питання щодо захисту інформації [124, с. 69].

Глобалізаційні процеси та інформатизація, які набувають великих всесвітніх масштабів, привели до відповідної реакції з боку міжнародної спільноти. Це виразилось у міжнародно-правових актах, спрямованих на врегулювання основних положень функціонування зазначених процесів. Серед основоположних документів, прийнятих міжнародним товариством у галузі інформатизації, необхідно виокремити такі: Окінавську хартію глобального інформаційного суспільства, Конвенцію про захист осіб стосовно автоматизованої обробки даних особистого характеру, Директиву 95/46/ЄС Європейського Парламенту та Ради Європи «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», Угоду про співробітництво в галузі інформації й інші документи [151, с. 673].

Головним поміж вказаних документів є Окінавська хартія глобального інформаційного суспільства, що прийнята 22 липня 2000 року. Вона акцентує увагу на тому, що інформаційно-комунікаційні технології є одним із найважливіших чинників, які здійснюють свій вплив на формування суспільства у XXI ст. Більше того, цей документ формує обсяг завдань, виконання яких є важливим для побудови інформаційного суспільства. З огляду на розвиток процесів глобалізації та інформатизації суспільства, цей процес супроводжується проникненням кримінальних структур у вказані сфери життя громади, суспільства, держави. При цьому підписанти Хартії прийняли на себе зобов’язання щодо забезпечення виконання ефективних заходів у боротьбі зі злочинністю в комп’ютерній сфері.

Суттевим кроком щодо розвинення інформаційного суспільства стала Всесвітня зустріч, яка проходила на вищому рівні у два етапи та стосувалася питань інформаційного суспільства. Спочатку зусріч провели у Женеві в 2003 році, а потім у Тунісі в 2005 році.

Результатом зустрічі в Женеві 12 грудня 2003 року стало ухвалення Женевської Декларації принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» та Женевського плану дій. Водночас у Тунісі з 16 по 18 листопада 2005 року були прийняті подальші зобов'язання щодо питань інформаційного суспільства.

Також доцільно розглянути Конвенцію про кіберзлочинність. Передумовою прийняття Конвенції стало проникнення кримінальних структур у сферу високих інформаційних технологій та їх використання для злочинної діяльності. У преамбулі Конвенції зазначено, що країни – члени Ради Європи й інші держави, які підписали Конвенцію, стурбовані ризиком того, що електронна інформація й комп'ютерні мережі можуть бути використані для вчинення кримінальних правопорушень, а докази, пов'язані з такими правопорушеннями, можуть зберігатись і передаватись комп'ютерними мережами [4].

Проаналізувавши глобальні тенденції, можна зробити висновок про те, що міжнародна юридична практика розробила декілька разових підходів щодо правового регулювання світового інформаційного простору. У цьому контексті потрібно виділити «азіатський» підхід, який являє собою всеосяжний контроль з боку держави над усіма правовідносинами в сфері інформації, наявність жорсткої цензури інформаційних ресурсів у кордонах політичної ідеології країни, зведення нанівець саморегулювання таких відносин відповідними учасниками інформаційної діяльності. Інший підхід має назву «європейський» та має в своїй основі європейські принципи свободи користування будь-яким способом інформаційними ресурсами без будь-яких обмежень. Такому підходу характерні значна саморегуляція інформаційних відносин між такими суб'єктами, регулювання державою

лише найбільш важливих положень, які побудовані на загальних принципах і технічних стандартах інформаційної діяльності.

У зв'язку з тим що всесвітня мережа Інтернет є таким собі інтернаціональним феноменом, який обов'язково таким чи іншим чином робить залежним від сфери інформаційних технологій усі країни. Тобто на сьогодні існує потреба в розробці уніфікованого законодавства. Одним із ефективних способів нормалізації національних законодавств є підготовка модельних законів, які містять у собі основні принципи, вироблені міжнародним правом. Особливістю цих актів є те, що вони не обов'язкові для виконання, а тільки напрявляють держави на основні концептуальні положення, яких потрібно дотримуватися під час розроблення та прийняття аналогічних національних законів.

Перший важливий крок у цьому напрямі зроблено Парламентською Асамблеєю країн СНД, яка ухвалила проект модельного закону «Про Інтернет». Головними проблемами, які повинні бути вирішені у вказаному законі, є такі: визначення основних понять: «Інтернет», «управління Інтернетом», «доменне ім'я», «сайт» (ст. 2); виокремлення учасників правовідносин у мережі Інтернет (ст. 3); розроблення низки вимог і положень протидії використанню мережі Інтернет у неправомірних цілях (ст. 13); дослідження місця та часу здійснення злочинних дій (ст. 11).

Україна має два напрями міжнародної співпраці у сфері інформаційної безпеки – СНД та ЄС. Доцільність такої співпраці пояснюється необхідністю встановлення взаємозв'язків шодо обміну інформацією між цими державами, для чого повинні були дотримані вказані умови.

Пріоритетними напрямами співпраці з ЄС є дотримання прав людини і засобів масової комунікації, суспільне телерадіомовлення, аудіовізуальна сфера, охорона інтелектуальної власності, боротьба з комп'ютерною злочинністю, захист суспільної моралі та запобігання насильству через програми, інформацію та ідеї, правове регулювання нових комунікаційних послуг [100, с. 11].

Крім того, можна застосувати міжнародний обмін інформацією в сфері податків і зборів, який буде здійснюватися через оформлення спеціальних запитів щодо одержання або надання інформації від інших суб'єктів з-за кордону. Звичайно це запит щодо інформації, яка може бути представлена внаслідок перевірки або розслідування діянь платників податків чи зборів, у тому числі відносно ухилення від їх сплати або щодо інших порушень законодавства, а також відповідно до контролю за дотриманням законодавства про податки, обов'язок щодо якого покладено на ці органи. Відповідний запит виконується у випадку, коли певні факти знаходять своє підтвердження про те, що потрібно отримати необхідну інформацію, яка перебуває за межами України. Тому звичайно певні зусилля зосереджені для отримання відповідної інформації, в тому разі, коли отримання такої інформації з джерел в Україні не дозволило досягти бажаного результату. Форма та зміст відповідного запиту щодо одержання або представлення інформації з-за кордону встановлюється міжнародними угодами. У разі коли форму та зміст такого запиту не встановлено, запит може бути сформований за взаємною домовленістю відповідних органів та виконаний лише за наявності міжнародних угод, якими передбачено такий обмін інформацією.

Обмін податковою та митною інформацією регулюється міжнародними юридичними інструментами: 1) двосторонніми податковими конвенціями, що базуються на типових Конвенціях ОЄСР і ООН про уникнення подвійного оподаткування щодо податків на дохід і капітал; 2) міжнародними інструментами, спеціально розробленими для цілей адміністративної взаємодопомоги з податкових питань; 3) у межах Європейського Союзу – Директивою ЄС про взаємну допомогу з питань обміну інформацією щодо ПДВ і акцизних зборів; 4) міжнародними угодами про допомогу в судових справах, наприклад Європейська конвенція про взаємну допомогу з кримінальних питань у випадках кримінального переслідування за податкові злочини [72, с. 416].

У 2001 році Європейською Комісією було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» (Network and Information Security: Proposal for A European Policy Approach), в якому окреслено європейський підхід до проблеми інформаційної безпеки. У документі використано термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надають через ці мережі і системи [168].

Залежно від напрямів злочинної діяльності, дії, що порушують безпеку інформаційних мереж і систем, поділяють на:

– викрадення електронних листів, збереження та перетворення даних;

– незаконний доступ до комп'ютера або інформаційних мереж;

– напади на сайти, домена, блокування роботи мереж адміністративного значення;

– віруси у мережі Інтернет;

– створення фальшивих сайтів.

До цих чинників також включається природні катаклізми, збої в мережі та помилки операторів, що мають серйозні наслідки.

Європейське співтовариство визначає мережу та інформаційну безпеку як головний елемент у розвитку інформаційного суспільства, важливим є наявність у них конфіденційної інформації та цінних економічних даних, що стимулює хакерів до нападу. Напади на інформаційні мережі прирівнюють по силі мережевих збоїв або згаданих вище природних катаклізмів та безпосередньо впливають на систему захисту інформації.

Найгірше, що може статися після атак – потенційні збитки порушення мережевої безпеки, ніхто не зможе оцінити, адже немає засобів для оповіщення. Такі атаки, хоча і впливають на нематеріальну сферу, можуть завдати репутаційних збитків, коли компанії не хочуть зайвого «чорного

піару». В умовах безперервного розвитку інформаційних технологій постійно виникають нові загрози, що викликають резонанс і потребують швидкого відгуку.

Раніше було оприлюднено такі засоби щодо забезпечення європейської політики інформаційної безпеки:

1. Створення освітньої системи щодо навчання користувачів використовувати інформаційні мережі.

Головна мета країн ЄС – надати громадянам країни, бізнес-партнерам та державним органам інформацію про мережеву та інформаційну безпеку. Запропоновано, зокрема, таке:

– країни-учасники повинні забезпечити створення інформаційно-освітньої кампанії для суспільства;

– країни-учасники повинні застосовувати нові стандарти безпеки, як ISO/IEC 17799;

– країни-учасники повинні влаштувати розгляд предметів у вищих та середніх навчальних закладах щодо питань безпеки в мережах.

2. Створення європейської системи попередження та інформування про нові загрози.

Основне завдання країн ЄС – створити систему попередження для користувачів, яка б не лише інформувала про небезпеку, але й давала поради щодо протидії атакам, а також створити конфіденційний механізм сповіщення про атаки для бізнесових структур. На сьогодні у країнах-членах функціонують «Комп'ютерні групи швидкого реагування» (CERTs). Однак такі групи часто не мають потрібного обладнання і чітко визначених функціональних обов'язків. Крім того, CERTs в Європі залежать від політики Координаційного центру комп'ютерних груп швидкого реагування (CERT/CC), що фінансується американським урядом. Як наслідок, європейське співробітництво є обмеженим. Для вирішення цієї проблеми пропонують такі дії:

– перегляд країнами-членами системи CERT стосовно технічного забезпечення та компетенції;

– створення зв’язку CERT мережі Євросоюзу з подібними структурами інших країн;

– обговорення з країнами-членами питання щодо організації на європейському рівні збору даних, аналізу та планування схем реагування на існуючі і потенційні загрози безпеці.

3. Забезпечення технологічної підтримки.

Пріоритетне значення надається розвитку досліджень з проблеми мережевої та інформаційної безпеки. Для цього запропоновано включати питання безпеки у Рамкові програми ЄС, а країнам-членам рекомендовано активно просувати використання засобів змінного стійкого шифрування.

4. Підтримка ринково орієнтованої стандартизації та сертифікації.

Підвищення безпеки інформаційних систем можливе за умови використання всіми суб’єктами єдиних стандартів. На сьогодні в ЄС працює Організація європейського співробітництва з питань акредитації (European cooperation for accreditation), яка несе відповідальність за сертифікацію бізнес-процесів та управління інформаційною безпекою. Діяльність Європейської ініціативи з питань стандартизації електронних підписів (European Electronic Signatures Standardisation Initiative) полягає у розробці єдиних рішень з метою підтримки директиви ЄС про електронні підписи, а також ініціативи впровадження інфраструктури з відкритими ключами (Public Key Infrastructure) [104, с. 33].

З цією метою Комісія пропонує вжити таких заходів:

– європейські організації зі стандартизації мають прискорити роботу над сумісними і безпечними продуктами і послугами;

– країни-члени мають просувати використання процедур сертифікації та акредитації по загальноприйнятих європейських та міжнародних стандартах, сприяючи взаємному визнанню сертифікатів;

– європейські комерційні організації мають брати більш активну участь в європейській (CEN, Cenelec, ETSI) та міжнародній діяльності зі стандартизації;

– країни-члени мають переглянути існуючі стандарти безпеки.

5. Правове забезпечення.

Пріоритетними напрямами політики ЄС у сфері правового регулювання інформаційної безпеки є захист персональних даних, телекомунікаційні послуги та кіберзлочинність. Для вдосконалення правової бази в сфері інформаційної безпеки Європейська Комісієя пропонує такі заходи:

– забезпечення спільного розуміння правових наслідків безпеки в електронних комунікаціях;

– створення країнами-членами сприятливих умов для вільного обігу продуктів і послуг шифрування через гармонізацію адміністративних експортних процедур та послаблення експортного контролю;

– розробка Комісією правових заходів для зближення національних законодавств щодо атак на комп'ютерні системи.

6. Зміцнення безпеки на державному рівні.

Проблема безпеки має важливе значення для подальшого розвитку е-урядування. За цих умов завданням державних органів влади є не лише забезпечення відповідності інформаційно-комунікаційних систем вимогам безпеки, але й сприяння розвитку культури безпеки, що передбачає розробку «організаційної політики безпеки». За цим напрямом передбачається реалізація таких заходів:

– країни-члени мають впровадити ефективні та сумісні засоби інформаційної безпеки як основу е-урядування та електронних державних закупівель;

– країни-члени мають використовувати електронні підписи під час надання державних онлайн послуг;

– Європейська Комісія має вжити заходів для посилення вимог безпеки для своїх інформаційно-комунікаційних систем.

7. Розвиток міжнародного співробітництва з питань інформаційної безпеки [171].

Головне завдання ЄС полягає у зміцненні взаємодії Європейської Комісії з міжнародними організаціями щодо врегулювання питань мережевої безпеки.

Європейська агенція з питань мережевої та інформаційної безпеки (ENISA), утворена ще 2004 року, займається сприянням та розвитком європейської спільноти та країн-учасників. Основними напрямами діяльності Агенції є:

– надання консультацій та допомоги Комісії і країнам-членам у сфері інформаційної безпеки;

– збір та аналіз даних щодо безпекових інцидентів в Європі та ризиків, що виникають;

– розробка методів оцінки та управління ризиками для підвищення здатності ЄС реагувати на загрози інформаційній безпеці;

– підвищення обізнаності та розвиток співробітництва між різними учасниками в сфері інформаційної безпеки, зокрема внаслідок стимулювання взаємодії між державним і приватним секторами. Агенція також допомагає Європейській Комісії у попередній технічній роботі для оновлення і вдосконалення європейського законодавства в сфері мережевої та інформаційної безпеки [174].

Дослідження роботи цієї Агенції показало, що їхня діяльність побудована на щорічних робочих планах/програмах, які містять перелік основних пріоритетів та заходів для досягнення поставлених цілей. Робота Агенції розподілена за такими стратегічними напрямами [174]:

1) надання підтримки зусиллям зацікавлених сторін у створенні довідника з практики сповіщення про інциденти;

2) підвищення здатності європейських електронних мереж протистояти зовнішнім впливам;

3) надання допомоги провайдерам у зміцненні стійкості їхніх мереж через проведення аналізу правових і політичних перешкод в обміні інформацією та визначення критеріїв стійкості систем;

4) створення сприятливих умов для проведення європейських тренінгів з питань інофрмаційної безпеки тощо;

5) визначення нових небезпек у сфері інформаційної безпеки і формування довіри;

6) розвиток співробітництва між країнами-членами.

ENISA посприяла забезпеченню співпраці між приватними і державними структурами щодо поширення інформації про правопорушення в мережі між фінансовим сектором і державними органами через Центри фінансової інформації та аналізу (FI-ISAC).

Діяльність Агенції спрямована на розвиток взаєморозуміння між особами, зацікавленими у реагуванні на нові загрози та ризики. Агенцією у 2008 – 2009 роках створено структуру, яка дає можливість зацікавленим сторонам більш ефективно ідентифікувати й розуміти поточні, а також майбутні ризики (Emerging and Future Risks), що виникають унаслідок впровадження новітніх інформаційних технологій. Крім того, Агенцією започатковано Форум з питань безпеки й створено експертні групи для надання оцінки й аналізу відповідних проблем [171].

Одним з пріоритетних напрямів діяльності Сьомої Рамкової програми ЄС були питання інформаційної безпеки (2007 – 2013 рр.). Дослідження проблемних питань безпеки інформаційних технологій у Сьомій Рамковій Програмі спрямовані на розвиток і підвищення рівня знань, технологій з метою розбудови відкритого інформаційного суспільства в Європі, де особистості та організації мають змогу повною мірою користуватися перевагами інформаційних технологій. Акцент зроблено на підвищенні

можливостей користувачів керувати й захищати свої інформаційні засоби, ідентичність та персональні дані у цифровому середовищі [173].

Політичні пріоритети в сфері інформаційної безпеки, визначені керівними органами Європейського Союзу, втілюються у життя на національному рівні як органами державної влади, так і неурядовими організаціями.

Однією з країн-лідерів ЄС за показниками розвитку інформаційного суспільства є Фінляндія. У рейтингу країн ЄС Фінляндія займає перше місце за рівнем цифрової грамотності (понад 50 % населення), друге місце – за показником поширення мережі широкосмугового зв'язку (34 % населення) [171].

Серед членів ЄС, а саме країн Центрально-Східної Європи, Естонія займає провідне місце у розробці, впровадженні та реалізації політики інформаційної безпеки. Таку політику інформаційної безпеки здійснює Міністерство економіки та комунікацій, а саме його структурний підрозділ – Департамент державної інформаційної системи та Естонський центр інформатики [67].

Основним завданням Департаменту державної інформаційної системи є налагодження політичної діяльності у галузі інформаційних технологій, створення плану заходів у сфері впровадження державних інформаційних систем.

Естонський центр інформатики є виконавчим органом у загальній системі державної інформаційної політики й розвитку державного сектору інформаційних технологій. Головними функціями Центру є координування розробки та здійснення керування державною інформаційною системою. Компетенцією Центру є: управління проектами, в тому числі підготовка IT-проектів для державних інституцій; здійснення моніторингу ситуацій з інформаційними технологіями; вироблення державних реєстрів; забезпечення функціонування комп'ютерних мереж; вироблення

нормативно-правових підстав для галузі інформаційних технологій; проведення державних закупівель інформаційних технологій та інші [168].

Міністерством економіки та комунікацій Естонії розроблено національну політику інформаційної безпеки. Основна мета політики Естонії в сфері інформаційної безпеки – створення безпечного і відкритого для міжнародної співпраці інформаційного суспільства. Головними завданнями є ліквідація загроз і безпека прав особи та забезпечення освіченості у цій сфері, проведення тренінгів у сфері інформаційної безпеки, участь у міжнародних ініціативах з е-безпеки, а також підвищення конкурентоспроможності економіки. Державна політика в сфері інформаційної безпеки охоплює п’ять сфер:

1. Співробітництво з питань е-безпеки, що координується Міністерством економіки та комунікацій. До сфери їх діяльності належать координація аналізу ризиків естонського ІКТ-середовища, створення і управління естонською комп’ютерною групою швидкого реагування, участь у діяльності Європейської агенції з питань мережевої та інформаційної безпеки, а також координація транскордонних ініціатив.

2. Кризовий менеджмент і кіберзлочинність, що координується Міністерством внутрішніх справ спільно з Міністерством оборони. Ця сфера діяльності включає підготовку плану державного кризового управління, координацію роботи державних і локальних кризових комітетів та координацію міжнародних ініціатив з кіберзлочинності.

3. Освіта і навчання, що координуються Міністерством освіти і науки, Міністерством оборони, Міністерством економіки і комунікацій та Державною канцелярією. Діяльність у цій сфері включає здійснення заходів зі зв’язків з громадськістю, проведення тренінгів, створення інформаційних веб-сайтів, розвиток співпраці зі школами тощо.

4. Безпечне е-урядування, що базується на відповідному законодавстві, стандартах та процедурах, таких як безпекові вимоги до баз даних, послуг та

державних закупівель. Нормативні питання узгоджує Міністерство економіки і комунікацій спільно з Міністерством внутрішніх справ.

5. Сфера додатків, що координується Міністерством внутрішніх справ та Міністерством оборони. До них належать координація завдань, пов'язаних з безпекою додатків, зокрема, розповсюдження ідентифікаційних карток (ID cards), використання інтегрованих засобів передачі й обробки інформації (телематики) в адміністративних мережах.

Щодо автоматизації процесів використання інформації, то світовим лідером у сфері автоматизації урядових інституцій є Канада. Розпочалися ці процеси з урядової ініціативи Government On-Line (GOL), що законодавчо відрегульована актом про доступ до інформації (Access to Information Act), прийнятим ще у 1983 р. Це фактично є системою електронного уряду, що впроваджується ще з кінця минулого століття і базується на всебічній інформатизації як органів влади, так й інших державних установ.

Фундаментальним дослідженням цих проблем, зокрема реалізації прав доступу громадян до урядової інформації в Канаді та в інших країнах, збіркою рекомендацій для вдосконалень цього процесу є Звіт Цільової групи з огляду доступу до інформації (Access to Information Review Task Force), що була створена за рішенням уряду. Ключовим моментом цього документа, що став керівним при створенні систем е-уряду в різних країнах, є забезпечення своєчасного і адекватного опрацювання в урядових агенціях запитів громадян з усіх питань (request processing) [68, с. 30].

Упродовж останніх років міжнародне співтовариство направило свої зусилля на боротьбу із кіберзлочинністю. Наприклад, на 53-й сесії ГА ООН було ухвалено Резолюцію «Досягнення у сфері інформатизації та телекомунікації у контексті міжнародної безпеки». У цьому документі акцентовано увагу на тому, що необхідно проводити пошуки способів забезпечити належну інформаційну безпеку та стабільне функціонування світових інформаційних систем.

Відповідно до Резолюції ГА ООН 60/45 (2006 р.) [80] створювалися групи урядових експертів, діяльність яких спрямовувалася на пошук шляхів зміцнення безпеки глобальних інформаційних та телекомунікаційних систем з урахуванням існуючих та потенційних загроз у зазначеній сфері. За результатами їхньої діяльності було розроблено низку рекомендацій, якими, зокрема, запропоновано: продовжити діалог між державами з метою визначення міжнародних підходів до організації захисту стратегічно важливої національної і міжнародної інфраструктури; зміцнення довіри та зменшення ризиків, пов'язаних із використанням інформаційно-комунікаційних технологій у державному секторі; обміну інформацією про технології, принципи та передові методи забезпечення інформаційної безпеки тощо.

Наголошувалося на важливості обміну досвідом правотворчої діяльності з питань забезпечення безпеки інформаційно-комунікаційних технологій [78].

Крім ООН, питанням правового забезпечення інформаційної безпеки займаються й інші міжнародні організації. Так, за ініціативою так званої «Групи восьми» ухвалено Окінавську хартію глобального інформаційного суспільства (2000 р.) [4], в якій наголошувалося, що солідарна основа політики і дій в інформаційній сфері спроможна змінити методи взаємодії держав щодо сприяння глобальному соціальному та економічному розвитку. Підкреслено, що формування глобального інформаційного суспільства має супроводжуватися заходами, спрямованими на створення безпечного та вільного від злочинності кіберпростору.

Протягом саміту, який проходив у 2010 році під головуванням ОБСЄ, главами держав і урядів 56 держав-членів визначено необхідність досягти «більшої єдності цілей і дій у протидії новітнім транснаціональним загрозам». У підсумковій декларації, ухваленій за результатами даного саміту, було акцентовано увагу на тому, що загрози інформаційній безпеці країн є одними з новітніх транснаціональних загроз.

Радою Європи підготовлено Конвенцію про кіберзлочинність, яку було відкрито до підписання у листопаді 2001 року. Зазначену Конвенцію, яка набула чинності 1 липня 2004 року, станом на серпень 2013 року ратифікували 40 держав. Україна її підписала у квітні 2005 року, а ратифікувала у грудні 2006 року. Положення цього міжнародно-правового акта встановлюють, що держави «мають вжити таких законодавчих та інших заходів, необхідних для встановлення кримінальної відповідальності відповідно до їх внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це» (ст. 2) [4].

Наприклад, Велика Британія має потужну функціонуючу систему, яка виконує завдання щодо інформаційної безпеки країни. Закони цієї держави визначають не лише захист інформаційних прав та свобод громадян і громадських організацій, а й формують їхнє суттєве обмеження в певних випадках в інтересах національної безпеки. Так, існують закони «Про захист інформації», «Про збереження державної таємниці», «Про телекомунікації», а також Кодекс щодо практики доступу до урядової інформації. Зазанчений кодекс визначає порядок обмеження доступу до конфіденційної інформації, власником якої є держава. Крім того, Закон «Про захист інформації» адаптовано до вимог Директиви ЄС «Про захист інформації» (1998 р.).

Водночас, наприклад, Німеччина має діючу урядову програму «Федеральна підтримка нових комунікаційних та інформаційних технологій» (1994 р.). Регламент цієї програми встановлює відповідний контроль з боку міністерств за здійсненням фінансування новітних напрямів діяльності інформаційних центрів і служб. Так, програма «Info-2000» визначає посилення відповідальності федеральних земель при виконанні останніми контролю за змістом інформації. Федеральний закон «Про телекомунікації» (1991 р.) надає відповідним землям право на ліцензування діяльності, спрямованої на обмеження поширення інформації забороненого змісту (насильство, агресія, порнографія тощо), а закон «Про Інтернет» (1997 р.) формує певні обмеження щодо свободи поглядів та розкриття змісту

інформації, яка може призвести до політичної нестабільності. Федеративний уряд Німеччини у лютому 2011 р. прийняв Стратегію кібербезпеки, відповідно до якої встановлено посилення захисту інфраструктури стратегічного значення. У межах цієї стартегії визначено, що всі урядові органи, які вивчають проблеми кіберзлочинності, повинні взаємодіяти не тільки між собою, але й з приватним сектором.

Для забезпечення швидкого виявлення та локалізації небезпечних інцидентів у сфері інформаційних технологій передбачено створити Центр кіберреагування. До завдань цього органу віднесено також вироблення рекомендацій щодо вжиття заходів із забезпечення безпеки в інформаційній сфері. Йдеться також про створення Ради з кібербезпеки – нового органу на рівні державного секретаріату. Заслуговує на увагу те, що на саміті ОБСЄ у 2011 році Німеччина висловила готовність працювати над розробкою міжнародного документа, який би регулював поведінку держав у кіберпросторі та закріплював принципи посилення довіри, прозорості й безпеки [78, с. 24 – 28].

Наприклад, у Франції, в межах державної інформаційної політики було сформовано систему безпеки інформації та попередження комп'ютерних злочинів. Також були сплановані та реалізовані заходи, спрямовані на обмеження іноземної присутності в інформаційному просторі. Крім того, передбачено просування національних інтересів у франкомовні країни Африки, Азії та Латинської Америки. Особливу увагу акцентовано на гарантуванні безпеки національного інформаційного простору. Отже, Закон «Про електронні комунікації» визначає діяльність Міністерства внутрішніх справ та Міністерства оборони Франції в інформаційному та комп'ютерному просторах, спрямовану на забезпечення контролю за передачею інформації, в тому числі в радіочастотному просторі.

У проекті Концепції інформаційного протистояння в інформаційних та телекомунікаційних системах акцентовано увагу на необхідності сформувати межі віртуального інформаційного простору, а також вказано на необхідність

юридично закріпити відповідні механізми використання інформаційних технологій як у воєнний час, так і протягом мирного періоду. У зв'язку з цим було запропоновано розробити та ухвалити закон, який би був спрямований на формування протидії нанесенню шкоди інформаційній інфраструктури країни, а також на попередження вторгненню в інформаційний та віртуальний простір Франції.

У лютому 2011 року уряд Нідерландів ухвалив Національну стратегію кібербезпеки «Сила через співпрацю», якою передбачено створення Національної ради з кібербезпеки. Завданням цього органу буде забезпечення реалізації підходу, в основу якого покладено співробітництво державного та приватного секторів, а також різних наукових центрів. Передбачено також створити Національний центр з питань кібербезпеки, завданням якого є виявлення тенденцій та загроз інформаційній безпеці, а також сприяння подоланню наслідків інцидентів і кризових ситуацій у цій сфері [78, с. 30].

Інформаційна безпека є одним з найважливіших аспектів концепції безпеки Грузії. Для поліпшення правового регулювання у цій сфері урядом розроблено ряд законопроектів. Зокрема, у 2010 р. під егідою Міністерства юстиції Грузії створено Агентство з обміну даними, що несе пряму відповідальність за розробку та здійснення політики у сфері інформаційної безпеки у державному секторі [78, с. 23].

Водночас у Сполучених Штатах Америки сформована власна інформаційна політика з огляду на необхідність забезпечити порядок побудови інформаційних потоків у політичній, економічній та військовій сферах для гарантування балансу між державним контролем та свободою інформаційної діяльності. Була створена законодавча база для гарантування інформаційної безпеки. Було здійснено регламентацію основ такого гарантування у законах: «Про удосконалення інформаційної безпеки», «Про комп'ютерну безпеку», «Про комп'ютерне шахрайство і зловживання»; урегульовано інформаційні відносини та сформовано порядок доступу до закритої інформації (закон «Про свободу інформації», «Про таємницю»,

«Про право на фінансову таємницю», «Про охорону особистих таємниць» «Про висвітлення діяльності уряду»). Вказані нормативні документи формують правову основу для прийняття відповідних підзаконних нормативно-правових актів, які також мають своєю ціллю реалізацію єдиної державної політики у сфері інформаційної безпеки.

26 листопада 2003 р. Конгресом США ухвалено закон «Про внутрішню безпеку» (Home Security Act), відповідно до якого створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладено координацію діяльності державних органів і всіх приватних структур з питань забезпечення інформаційної безпеки. Цим законом передбачено розробку Національної стратегії із забезпечення безпеки у кіберпросторі (National Strategy to Secure Cyberspace) та Національної стратегії фізичного захисту об'єктів життєзабезпечення населення (The National Strategy for the Physical Protection of Critical Infrastructures). Зазначеними документами передбачено створення єдиної національної системи протидії кібернетичному тероризму, в рамках якої ініційовано створення територіальних, відомчих і приватних центрів протидії, визначено їхні функції та порядок взаємодії [78, с. 40].

Для забезпечення інформаційної безпеки в податковій та митній сферах США діє Прорама захисту платників податків Служби внутрішніх доходів США. Також у системі Служби внутрішніх доходів США (IRS) функціонує Організація з надання допомоги жертвам розкрадання особистої інформації (IDTVA). Вказаний орган здійснює захист конфіденційної інформації платників податків, зборів та проводить аналіз звітніх документів, поданих неналежним чином.

Факти витоку та розкрадання конфіденційної інформації платників податків виявляються Організацією з надання допомоги жертвам розкрадання особистої інформації під час опрацювання податкової декларації та проведення податкового аудиту в рамках Прорами захисту платників податків. У таких випадках Служба внутрішніх доходів США направляє

запит платнику податків для підтвердження його особистості протягом 30 днів. Після цього платник податків має підтвердити, чи подавав він податкову декларацію.

У разі якщо податкова декларація не подалавалася платником податків, вона буде видалена із податкової справи. Надалі жертва розкрадання конфіденційної інформації буде прийнята в програму особистих ідентифікаційних номерів для захисту особистої інформації (IP PIN) і буде щорічно отримувати новий шестизначний номер, який зазначається в податковій декларації. Такий ідентифікаційний номер забезпечує додатковий рівень захисту особистої інформації.

Крім того, якщо платник податків самостійно виявив дії з розкрадання конфіденційної інформації, то він може повідомляти Організацію з надання допомоги жертвам розкрадання особистої інформації Служби внутрішніх доходів США. У такому разі вживають таких заходів:

– податкова декларація, подана в електронній формі, не буде прийнята, оскільки вона дублює податкову декларацію, подану раніше;

– платник податків має: подати податкову декларацію у печатному вигляді, якщо немає можливості подати в електронній формі; заповнити заяву про розкрадання особистих даних.

Служба внутрішніх доходів США опрацьовує ці документи та направляє справу платника податків до Організації з надання допомоги жертвам розкрадання особистої інформації, де нею займаються співробітники, які пройшли спеціальну підготовку.

Організація з надання допомоги жертвам розкрадання особистої інформації, у свою чергу, вживає таких заходів протягом 120 днів, у важких випадках – 180 днів і більше:

– здійснюється оцінка обсягу проблем витоку особистої інформації та визначається, з якими податковими роками він пов’язаний;

– забезпечується пошук інших можливих жертв з-поміж осіб, вказаних у декларації, яка подана шахрайським шляхом;

– здійснюється повторна перевірка справжності чи хибності всіх імен, прізвищ, адрес та номерів соціального забезпечення, зазначених у декларації;

– видаляється з податкової справи платника декларація, подана шахрайським шляхом, та така справа позначається показником про розкрадання особистої інформації. Платнику податків направляється повідомлення про те, що його справа закрита.

До початку наступного періоду подання податкових декларацій платнику податків направляється лист з особистим ідентифікаційним номером для захисту конфіденційної інформації, за допомогою якого підпищується рівень захисту конфіденційної інформації.

Позитивний досвід США щодо створення Організації з надання допомоги жертвам розкрадання особистої інформації, яка функціонує в системі Служби внутрішніх доходів США, може бути запозичений Україною, а його реальне впровадження в національну юридичну практику дасть змогу більш дієво захистити конфіденційну інформацію платників податків.

Досвід Великої Британії, Німеччини свідчить про створення системи інформаційної безпеки з єдиним координуючим органом, який може за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії загрозам інформаційній безпеці та їх нейтралізації. Ці системи підпорядковуються главі виконавчої влади та, як правило, містять такі складові: 1) військову – для здійснення розвідувальних та оборонних операцій в інтересах збройних сил; 2) захисту критичної інфраструктури – для захисту інформаційно-телекомунікаційних систем органів державної влади, місцевого самоврядування, стратегічно важливих для держави підприємств, енергогенеруючих об’єктів, об’єктів транспорту, водо-, електро-, тепло- і газопостачання, життєзабезпечення та підвищеної небезпеки; 3) правоохоронну – для запобігання, виявлення, припинення та розслідування комп’ютерних правопорушень, притягнення зловмисників до відповідальності; 4) дорадчо-консультативну – для розроблення стратегії

державної політики та контролю виконання рішень керівництва держави у сфері протидії кіберзагрозам.

Незважаючи на деякі позитивні дії уряду України в інформаційній сфері, міжнародний досвід у боротьбі з загрозами інформаційної безпеки є необхідним для України, наприклад, у формуванні відповідної політики і побудові власної системи інформаційної безпеки.

Незважаючи на те що провідні країни світу розробили концепції національної стратегії щодо забезпечення інформаційної безпеки, що мають у собі принципи та пріоритети, завдання щодо досягнення зазначеної цілі, положення України залишається без стратегічного підгрунтя. Тобто на даний час країна має завдання створити стратегію підтримання безпеки за допомогою підходів і напрямів, як на міжнародному та національному рівнях.

Принципово, що Україна не тільки підписала 23.11.2001 року, а й ратифікувала 07.09.2005 року Конвенцію про кіберзлочинність, яка вступила в дію 01.07.2006 року [4]. Крім того, вона є активним учасником Комітету Конвенції з кіберзлочинності, який проводить щорічні зустрічі і визначає пріоритети подальшого поширення Конвенції, насамперед на країни, які входять до Ради Європи [169]. На сьогодні у законодавство України вже імплементовано ряд положень Конвенції про інформаційну безпеку. Крім того, є проекти про подальше їх впровадження, а також імплементацію.

Згідно з міжнародним досвідом, крім створення власної стратегії інформаційної безпеки, Україна потребує проведення комплексних навчальних програм з протидії тяжким злочинам у інформаційній сфері з метою, як практичної підготовки персоналу профільних відомств, так і налагодження зв’язків між інституціями, які відповідають за інформаційну безпеку держави. Крім навчання на національному рівні, бажаною є участь України у загальноєвропейських навчальних програмах з інформаційної безпеки. Доречним є ініціювання Україною таких навчальних програм і в межах програми «Партнерство заради миру».

На даний момент постає гостра потреба українському суспільству відігравати більшу роль у захисті даних у мережі Інтернет, що означає визначення «кібербезпеки» і «кіберозброєння». Важливим завданням є визначення базових понять питань кібербезпеки: «кібербезпека», «кіберпростір», «кібернапад», «кібервійна», «кібертероризм». Такі засоби повинні допомогти країні досягнути державі статусу інформаційно-розвиненої держави, що буде посідати важливе місце у міжнародному союзі та бути членом ЄС.

Створення реального міжнародного консенсусу з цього питання між лідерами-державами є об'єктивною необхідністю, оскільки унеможливить подальше стрімке зростання загроз інформаційній безпеці як на національному, так і міжнародному рівні.

Україна вже сьогодні відчуває вплив кіберзлочинності злочинності у сфері інформаційної безпеки і об'єктивно зацікавлена в тому, щоб брати у цих дискусіях активну участь, оскільки міжнародний досвід у боротьбі з загрозами інформаційної безпеки є необхідним для неї як приклад у формуванні відповідної політики і побудові власної системи інформаційної безпеки, насамперед унаслідок створення Стратегії. Адже з керівних документів державної інформаційної політики України, що визначають діяльність органів влади в інформаційній сфері, доктринально визначені тільки питання безпеки, а закони і основні принципи регулюють лише питання, пов'язані з новітніми інформаційними технологіями.

У світових державах та ЄС поняття інформаційної безпеки полягає у такому стані безпеки інформаційних мереж і систем, що забезпечує пітримку належного рівня захисту цілісності, доступності й конфіденційності інформації та відповідного рівня протидії зовнішнім та внутрішнім небезпекам. Отже, одним з пріоритетних напрямів зарубіжних країн та країн ЄС у інформаційній безпеці є створення і застосування комплексу різноманітних засобів, які сприятимуть підтримці безпеки та захисту інформаційно-комунікаційних технологій.

Важливим напрямом забезпечення безпеки у країнах ЄС та інших країнах світу є створення юридичних засад інформаційної безпеки, що означає розробку нормативно-правових актів, які б встановлювали перелік злочинів, пов'язаних із інформаційними технологіями, й визначали відповідну кримінальну відповідальність. Іншим пріоритетом політики ЄС та інших провідних країн світу є інформаційна безпека громадян. По суті, це високий рівень обізнаності громадськості щодо ризиків та загроз, пов'язаних з інформаційними технологіями та щодо способів захисту своїх інформаційних систем і мереж від небажаних впливів. Це включає в себе захист від злочинів у кібер-просторі та безпеку таких осіб, дослідження та утилізацію підозрілої інформації в Інтернеті. В Україні доцільно запровадити досвід роботи США, Великої Британії та Німеччини щодо створення єдиного координуючого органу, який зможе за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії загрозам інформаційній безпеці органів ДФС та їх нейтралізації.

## Висновки до розділу 3

У процесі дослідження зазначених вище питань було зроблено такі висновки:

1. Наголошено, що швидкий розвиток інформаційних технологій впливає на прийняття законодавчим органом України нормативно-правових актів, спрямованих на врегулювання обігу інформації та дотримання положень інформаційної безпеки, а також прав та сводоб людини і громадянина. Тому на сьогоднішні необхідно оперативно реагувати на зміни стандартів у цій сфері.

2. Особливим недоліком правового регулювання інформаційної безпеки органів ДФС України є розпорошення зазначеного питання у багатьох нормативно-правових актах.

3. Визначено, що вимоги інформаційної безпеки органів ДФС України повинні органічно включатися у законодавство, в тому числі і в конституційне, основні загальні закони, закони щодо організації державної системи управління, спеціальні закони, відомчі правові акти тощо.

4. Для забезпечення інформаційної безпеки органів ДФС України запроповано встановити інститут податкової й митної таємниці.

5. Головними шляхами функціонування та дотримання правового режиму інформації в органах ДФС України є: забезпечення юридичних та технічних можливостей щодо доступу, обробки, збереження та передавання інформації; гарантування захисту інформації в органах ДФС України; доступ до автоматизованих інформаційних систем органів ДФС України з дотриманням відповідних механізмів захисту інформації, яка до них вноситься; впровадження в діяльність органів ДФС новітніх інформаційних систем та технологій, а також вдосконалення їх захисту; прийняття оновлених державних програм, спрямованих на вдосконалення правового забезпечення обігу податкової й митної інформації в державі, враховуючи міжнародний досвід та положення європейського законодавства; збільшення

інформаційного обміну між національними органами та зарубіжними податковими й митними органами, що зумовлено транснаціональністю інформаційних правопорушень.

6. Питання нормативно-правового регулювання відповідних інформаційних відносин та інформаційної безпеки органів ДФС України визнано важливими та актуальними, адже здійснюється систематичне вдосконалення інформаційних ресурсів, налагодження інформаційних зв'язків з фізичним й юридичними особами (платниками податків, зборів), державними органами, владними органами іноземних країн і міжнародних організацій.

7. Проаналізовано нормативні засади та порядок організації інформаційної безпеки у США, Великій Британії, Німеччині, Естонії, Канаді, Франції, Нідерландах та визначено напрями запозичення такого досвіду для України. Визначено, що для України є позитивним досвід США, Великої Британії, Німеччини щодо створення системи інформаційної безпеки з єдиним координуючим органом, який зможе за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії загрозам інформаційній безпеці та їх нейтралізації у державних органах.

8. Не менш позитивним вбачається досвід Естонії щодо розробки, впровадження та реалізації політики інформаційної безпеки Департаментом державної інформаційної системи, який фукціонує в Міністерстві економіки та комунікацій. Основним завданням Департаменту державної інформаційної системи є налагодження політичної діяльності у галузі інформаційних технологій, створення плану заходів у сфері впровадження інформаційних систем у державні органи. Також виконавчим органом у загальній системі державної інформаційної політики й розвитку державного сектору інформаційних технологій є Естонський центр інформатики, який здійснює координацію розробки та керування державною інформаційною системою. З огляду на те, що в Україні відсутній єдиний державний орган, який би

забезпечував інформаційну безпеку в органах державної влади, зокрема в органах ДФС, досвід Естонії є перспективним для нашої держави. Створення такого органу в нашій країні надасть можливість більш ефективно забезпечувати органи ДФС провідними інформаційними системами й протидіяти загрозам, які виникають в інформаційній сфері держави.

# ВИСНОВКИ

У дисертаційному дослідженні виконано теоретичне узагальнення та запропоновано нове розв’язання наукового завдання, яке полягає у формулюванні науково обґрунтованих рекомендацій щодо наукового визначення сутності, змісту та способів забезпечення інформаційної безпеки під час виконання органами ДФС України своїх функцій, запропоновано напрями вдосконалення чинного законодавства та його застосування на практиці у вказаній сфері. Сформульовано висновки і пропозиції, спрямовані на вирішення зазначеного завдання, основні з яких такі.

1. Інформаційна безпека передбачає дієвий комплекс заходів, які повинні надійно захищати фінансово-економічну, соціальну, політичну й інші сфери дільності держави, інтелектуальну власність осіб, а також відомості, що становлять передбачену законом таємницю. В органах ДФС більшість функціональних підрозділів тією чи іншою мірою виконують завдання із забезпечення внутрішньої інформаційної безпеки. Встановлено, що на сьогодні існують певні загрози інформаційній безпеці ДФС щодо забезпечення конфіденційності податкової та митної інформації, несанкціонованого втручання в роботу інформаційних систем, позаслужбового використання відповідної інформації. Ефективний захист інформаційних систем і баз даних є запорукою сталого розвитку країни та забезпечення безпосередньої інформаційної безпеки органів ДФС України.

2. Процес управління в органах ДФС неможливий без накопичення відповідної інформації. Без належної інформації важко провести належну оцінку відповідної ситуації, виявити наявні проблеми, передбачити можливий перебіг дій, сформувати цілі, яких потрібно досягнути, сформувати та затвердити певні рішення щодо управління цими процесами та виконати контроль за їх реалізацією.

3. Встановлено, що під час виконання функціональних обов’язків органи ДФС використовують податкову та митну інформацію, правовий

режим якої закріплено у Податковому та Митному кодексах України. Запропоновано поняття «митна інформація» чітко визначити в Законі України «Про інформацію», зокрема у ст. 10, що надасть можливість уникнути суперечностей щодо порядку її використання та зберігання органами ДФС, у тому числі під час внесення до інформаційних систем і баз даних.

4. Виокремлено характерні риси інформаційної безпеки в органах ДФС України, якими є гарантування безпеки доступності комбінацій, цілісності та відповідної конфіденційності інформаційних баз даних. Підкреслено, що інформаційна безпека органів ДФС України побудована на діяльності щодо створення, підтримання й захисту на належному законодавчому та технічному рівнях інформаційних систем, також основних прав і свобод людини й громадянина.

5. Здійснено комплексне дослідження повноважень суб'єктів забезпечення інформаційної безпеки в органах ДФС України і конкретизовано їхні завдання та функції. Вивчення повноважень зазначених суб'єктів дозволило визначити, що їхні комплексні завдання та функції, спрямовані на гарантування інформаційної безпеки податкової та митної сфер держави, відображено не повною мірою. У зв'язку з цим запропоновано вдосконалити повноваження Головного управління внутрішньої безпеки ДФС України щодо виявлення і протидії інформаційним правопорушенням та розробити в інформаційно-телекомунікаційній системі «Податковий блок» підсистему «Електронний журнал безпеки», метою якого є зменшення можливості вчинення несанкціонованих дій посадовими особами ДФС України під час адміністрування податків, зборів та платежів. Ведення «Електронного журналу безпеки» дозволить фіксувати дії користувачів під час перегляду інформації, яка міститься в ІТС «Податковий блок». Використовувати підсистему «Електронний журнал безпеки» матимуть можливість лише співробітники внутрішньої безпеки.

6. Основними інформаційними ресурсами органів ДФС, які використовують під час поточної діяльності співробітники, є такі: інформаційна система «Податковий блок», до складу якої входять такі підсистеми: «Обробка податкових зобов'язань та платежів», «Облік платежів», «Податковий аудит», «Реєстрація платника податків», «Аналітична система»; автоматизована інформаційна система «Архів електронної звітності», у структурі якої діє інформаційна система «Єдиний реєстр податкових накладних»; автоматизована система митних оформлень «Інспектор»; інформаційна система «Галузь»; автоматизована інформаційна система «Управління документами».

7. Встановлено, що для вдосконалення інформаційного забезпечення управління в органах ДФС України потрібно вжити дієвих заходів, що проявляться у такому:

– організація захисту органами ДФС конфіденційної інформації про фізичних та юридичних осіб для недопущення несанкціонованого поширення такої інформації, а також забезпечення високого рівня адміністрування податків, зборів, обов'язкових платежів;

– розробці спеціальних програмних комплексів для виявлення та протидії несанкціонованому втручанню до інформаційно-телекомунікаційних систем органів ДФС;

– здійсненні систематичного аналізу податкових та митних ризиків, що можуть бути пов'язані зі здійсненням несанкціонованого втручання в роботу автоматизованих систем ДФС України, з метою оперативного реагування та координації діяльності структурних підрозділів з їх відпрацювання;

– виконанні аналітичної роботи відповідними підрозділами ДФС для визначення фактів протиправної діяльності у податковій та митній сферах;

– проведенні митних процедур з використанням інформаційних систем і засобів їх забезпечення.

8. З'ясовано, що інформаційні правовідносини в податковій і митній сферах держави становлять собою однорідну групу суспільних

відносин, які виникають під час виконання покладених на органи ДФС функцій та завдань щодо справляння податків та зборів, здійснення державної митної справи, а також щодо реалізації фізичними та юридичними особами права на податкову й митну інформацію.

9. Основними комплексними заходами захисту інформації й інформаційних відносин в органах ДФС України є: спеціальне діловодство; режим секретності, включаючи технічний захист інформації; технічний і криптографічний захист інформації; голографічний захист носіїв інформації; правовий та організаційний захист інформації як відокремлені види захисту, які передбачають порядок захисту, юридичну відповідальність, так і складові всіх інших видів (правову основу окремих різновидів захисту інформації).

10. Зазначено, що адміністративну відповідальність за вчинені інформаційні правопорушення потрібно розуміти як процедуру застосування до особи, яка визнана винною у вчиненні відповідних дій або бездіяльності та яка здійснила інформаційне правопорушення, конкретних заходів впливу відповідно до санкції порушеної правової норми, яка застосовується у встановленому випадку. Така норма є частиною системи інформаційного правопорядку, який формує правову основу інформаційного суспільства.

11. Визначено, що інформаційне правопорушення у діяльності ДФС України – це протиправна, винна (умисна або необережна) дія чи бездіяльність суб’єкта інформаційних відносин, який посягає на встановлений законодавством правопорядок у податковій чи митній сферах держави щодо обробки персональних даних, доступу до інформації, її захисту, а також посягає на функціонування інформаційних технологій та інформаційних ресурсів ДФС України, за яку законом передбачено юридичну відповідальність.

12. Встановлено, що особливим недоліком нормативно-правового регулювання інформаційної безпеки органів ДФС України є його розпорошення у великій кількості нормативно-правових актів. Характерною рисою національного інформаційного законодавства є декларативність

значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації правових норм, які регулюють суспільні відносини у сфері забезпечення інформаційної безпеки.

13. Обґрунтовано необхідність внести зміни до Податкового кодексу України, а саме:

– до статті 72 ПК України, в якій закріплено порядок збору податкової інформації. Додати до вказаної статті пункт 72.2, в якому викласти перелік податкової інформації, яка є службовою, та закріпити вимоги щодо її конфіденційності. А саме, запропоновано пункт 72.2 статті 72 ПК України викласти в такій редакції: «72.2.1. Службовою інформацією в органах ДФС є така: податкова інформація та інформація з питань податкових перевірок; з питань дотримання охорони державної таємниці, технічного та криптографічного захисту інформації; відомості стосовно інформатизації; інформація, що стосується роботи з особовим кадровим складом; інформація, отримана під час здійснення правоохоронної діяльності; відомості стосовно мобілізаційної роботи та цивільного захисту; інформація, яка опрацьовується не секретним діловодством; митна інформація.

72.2.2. За несанкціоноване розголошення відомостей, які містять службову інформацію, посадові особи органів ДФС несуть відповідальність, передбачену чинним законодавством.

72.2.3. Відомості, які містять у собі службову інформацію, надаються розпорядником інформації, якщо він правомірно раніше її оприлюднив.

72.2.4. Службова інформація має надаватися розпорядником інформації, якщо відсутні законні підстави для обмеження у доступі до вказаної інформації, що існували раніше.

72.2.5. Конфіденційна інформація, яку збирають, використовують і формують органи ДФС, розголошується з дозволу фізичної або юридичної особи, які є власниками такої інформації.

Конфіденційна інформація може поширюватися тільки за згодою осіб, які обмежили доступ до такої інформації, а у разі відсутності згоди – тільки в інтересах національної безпеки, економічного добробуту та прав людини».

14. На підставі аналізу правового забезпечення інформаційної безпеки фіскальних органів зарубіжних країн встановлено, що координуючі органи систем інформаційної безпеки цих країн здатні за короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії загрозам інформаційній безпеці та їх нейтралізації у державних органах. Позитивний досвід США щодо створення Організації з надання допомоги жертвам розкрадання особистої інформації, яка функціонує в системі Служби внутрішніх доходів США може бути запозичений Україною, а його реальне впровадження в національну юридичну практику дасть змогу більш дієво захистити конфіденційну інформацію платників податків.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

***Нормативно-правові акти:***

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

2. Загальна декларація прав людини: Декларація ООН, Міжнародний документ від 10.12.1948 р. [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

3. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950 р. [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

4. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 р. [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

5. Податковий кодекс України: Закон України від 02.12.2010 р. № 2755-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

6. Митний кодекс України: Закон України від від 13.03.2012 р. № 4495-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

7. Цивільний кодекс України: Закон України від від 16.01.2003 р. № 435-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

8. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

9. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

10. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 р. № 537-V [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

11. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

12. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

13. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

14. Про науково-технічну інформацію: Закон України від 25.06.1993 р. № 3322-XII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

15. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23.09.1997 р. № 538/97-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

16. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

17. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

18. Про збір та облік єдиного внеску на загальнообов’язкове державне соціальне страхування: Закон України від 08.07.2010 р. № 2464-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

19. Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців: Закон України від 15.05.2003 р. № 755-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

20. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

21. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

22. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

23. Про затвердження порядку ведення Єдиного реєстру податкових накладних: Постанова Кабінету Міністрів України від 29.12.2010 р. № 1246 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

24. Про державну таємницю: Закон України від 21.01.1994 р. №3855-XII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

25. Про інформаційні агентства: Закон України від 28.02.1995 р. № 74/95-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

26. Про радіочастотний ресурс: Закон України від 01.06.2000 р. № 1770-III [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

27. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

28. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

29. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

30. Про захист економічної конкуренції: Закон України від 11.01.2001 р. № 2210-III [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

31. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

32. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

33. Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

34. Витяг з додатку до Постанови Верховної Ради України від 04.12.2014 р. № 22–VIII [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

35. Про затвердження плану заходів із створення інтегрованої міжвідомчої інформаційно-телекомунікаційної системи щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон: Розпорядження Кабінету Міністрів України від 19.04.2006 р. № 215-р [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

36. Про затвердження Положення про Державний комітет телебачення і радіомовлення України: Постанова Кабінету Міністрів України від 13.08.2014 р. № 341 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

37. Про затвердження Положення про Державну фіскальну службу України: Постанова Кабінету Міністрів України від 21.05.2014 р. № 236 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

38. Про затвердження Порядку періодичного подання інформації органам державної податкової служби та отримання інформації зазначеними органами за письмовим запитом: Постанова Кабінету Міністрів України від 27.12.2010 р. № 1245 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

39. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

40. Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади: Постанова Кабінету Міністрів України від 28.10.2004 р. № 1453 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

41. Питання Національного інституту проблем міжнародної безпеки: Указ Президента України від 29.07.1997 р. № 719/97 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

42. Про затвердження Доктрини інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

43. Про Міжвідомчу комісію з питань інформаційної національної безпеки і оборони України: Указ Президента України від 22.01.2002 р. №63/2002 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

44. Про Національну комісію, що здійснює державне регулювання у сфері зв`язку та інформатизації: Указ Президента України від 23.11.2011 р. № 1067/201 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

45. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

46. Стратегія національної безпеки України: Указ Президента України від 26.05.2015 р. № 287/2015 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

47. Порядок взаємодії між Єдиним державним реєстром юридичних осіб та фізичних осіб – підприємців та інформаційними системами Державної фіскальної служби України, обміну документами в електронній формі: Наказ Міністерства юстиції України, Міністерства фінансів України від 09.10.2015 р. № 1918/5/869 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

48. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби безпеки України від 12.08.2005 р. № 440 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

49. Про затвердження Інструкції щодо порядку збору, обробки та надання оперативної інформації підрозділами оперативного реагування: Наказ ДПА України від 14.01.2010 р. № 17 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

50. Про затвердження Стратегічного плану розвитку ДФС України на 2015-2018 роки: Наказ ДФС України від 12.02.2015 р. № 80 [Електронний ресурс]. – Режим доступу: http://sta-sumy.gov.ua.

51. Про затвердження Переліку відомостей, що містять службову інформацію та яким присвоюється гриф обмеження доступу «Для службового користування» в органах ДФС України: Наказ ДФС України від 28.08.2014 р. № 88 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

52. Про затвердження форми запиту на інформацію, Інструкції щодо процедури подання запиту на інформацію, її отримання в ДПА України та Порядку складення та подання запитів на інформацію ДПА України: Наказ Державної податкової адміністрації України від 08.06.2011 р. № 345 [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

***Спеціальна література:***

53. Абакумов В. М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони / В. М. Абакумов // Форум права. – 2012. – № 4. – С. 10–16.

54. Аблякимов Е.Е. Правові основи формування державних електронних інформаційних ресурсів: дис. … канд. юрид. наук: 12.00.07 / Аблякимов Е.Е. – Київ, 2010. – 204 с.

55. Административная ответственность : учебн.-практ. пособие / Э. Г. Липатов, А. В. Филатова, С. Е. Чаннов; под. ред. С. Е. Чаннов. – М.: Волтерс Клувер, 2007 [Электронный вариант]. – Режим доступа: www.consultant.ru.

56. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: [монографія] / І.В. Арістова; за заг. ред. О.М. Бандурки. – Харків: Вид-во Ун-ту внутр. справ, 2000. – 368 с.

57. Архипова Є.О. Соціально-філософське осмислення поняття «інформаційна безпека» / Є.О. Архипова // Вісник НТУУ – КПІ. Філософія. Психологія. Педагогіка. – 2011. – Випуск 3. – С. 7–11.

58. Афанасьев В.Г. Социальная информация / В.Г. Афанасьев – М.: Наука, 1994. – 201 с.

59. Бабін І. І. Правове регулювання податкової таємниці за законодавством України / І. І. Бабін // Науковий вісник Чернівецького університету. – 2012. – № 618. – С. 98–101.

60. Бачило И.Л. Информационное право. Роль и место в системе права Российской Федерации / Бачило И.Л. // Государство и право. – 2001. – № 2. – С. 5–14.

61. Бачило И.Л. Информация как предмет правоотношений / И.Л. Бачило // Науч. техн. Информация – 1997. – № 9. – С. 17–25. – (Серия 1).

62. Безрученко В.С. Інформація та інформаційні ресурси як елементи інформаційного забезпечення правоохоронної діяльності податкової міліції / В.С. Безрученко, Д.О. Мороз // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матер. наук.-практ. конф. (24 грудня 2010 р.); Львівський державний університет внутрішніх справ. – Львів, 2010. – С. 333–338.

63. Беляков К.И. Управление и право в период информатизации: монография / Беляков К. И. – К. : КВІЦ, 2001. – 308 с.

64. Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні: автореф. дис. на здобуття наукового ступеня кандидат юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / І. Р. Березовська. – Київ, 2012. – 20 с.

65. Березовська І.Р. Поняття і характеристика структурних елементів механізму застосування адміністративно-правових засобів забезпечення інформаційної безпеки України / І.Р. Березовська // Науковий вісник національної академії внутрішніх справ. – 2013. – № 2. – С. 31–35.

66. Блищик Л.П. Інформаційне забезпечення діяльності суб'єктів податкових правовідносин / Л.П. Блищик // Науковий вісник Національного університету ДПС України (економіка, право). – 2012. – № 2 (57). – С. 163–168.

67. Бондар Ю. В. Енциклопедія для видавця та журналіста / Ю.В. Бондар, М. Ф. Головатий, М. І. Сенченко // МАУП, Книж. палата України. – К.: ДП «Вид. дім «Персонал», 2010. – 400 с.

68. Брижко В.М. Інформаційне суспільство. Дефініції / В.М. Брижко, О.М. Кальченко, В.С. Цимбалюк; за ред. Р.А. Калюжного, М.Я. Швеця. – К.: Інтеграл, 2002. – С. 86.

69. Брижко В.О. До питання сучасної інформаційної політики / В.О. Брижко // Вісник Академії управління МВС. – 2009. – № 2. – С. 27–46.

70. Воскресенский Г.М. Теория и практика информационного обеспечения управления в органах внутренних дел / Г.М. Воскресенский. – М., 1985. – С. 21.

71. Гаврилов О.А. Информатизация правовой системы России. Теоретические и практические проблемы: [учеб. пос.] / Гаврилов О.А. – М.: Юридическая книга: ЧеРо, 1998. – С. 52–53.

72. Гальчинський А.С. Стратегія економічного і соціального розвитку України (2004–2015 роки). Шляхом Європейської інтеграції / А.С. Гальчинський, В. М. Геєць. – К.: ИИЦ Госкомстата Украины, 2004. – С. 416.

73. Годун В.М. Інформаційні системи і технології в статистиці : Навч. посібник / В.М. Годун, Н.С. Орленко; за ред. В.Ф. Ситника. – К.: КНЕУ, 2003. – 267 с.

74. Головань С.М. Про термінологію в області безпеки інформації / С.М. Головань, А.М. Давиденко, Л.М. Щербак // Моделювання та інформаційні технології: зб. наук. пр. – К.: ІПМЕ ім. Г.Є.Пухова НАН України, 2010. – Вип. 57. – С. 37–41.

75. Гребенюк О.В. Визначення рівня тіньової економіки в контексті формування і розвитку системи інформаційної безпеки України / О.В. Гребенюк // Економіка промисловості. – 2010. – № 1. – С. 68–71.

76. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання / В. Гурковський // Вісник Української академії державного управління при Президентові України. – К. , 2002. – № 3. – С. 27–32.

77. Дмитренко Е.С. Повноваження органів державної податкової служби у сфері забезпечення інформаційної безпеки: проблеми реалізації / Е.С. Дмитренко // Інформаційна безпека людини, суспільства, держави. – 2012. – № 1 (8). – С. 41–46.

78. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201) // Нью-Йорк, Организация Объединенных Наций. – 2012. – 57 с.

79. Долгий О.А. Класифікація інформації: зв’язок із забезпеченням безпеки працівників державної податкової служби / О.А. Долгий // Підприємництво, господарство і право. – 2003. – № 11. – С. 75–79.

80. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеей ООН от 06.01.2006 (A/RES/60/45) [Електронний ресурс]. – Режим доступу: https://www.un.org/disarmament/ru.

81. Електронне оподаткування: сутність та перспективи застосування: монографія / [П.В. Мельник, А.М. Новицький, О.А. Долгий та ін.] ; за заг. ред. П. В. Мельника. – Ірпінь : Національний університет ДПС України, 2010. – 332 с.

82. Енциклопедичний словник з державного управління / уклад.: Ю.П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін.; за ред. Ю.В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. – К.: НАДУ, 2010. – 820 с.

83. Зайцев М.М. Суб'єкти забезпечення інформаційної безпеки України / М. М. Зайцев // Форум права. – 2013. – № 3. – С. 231–238.

84. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения: ГОСТ 34.003-90 [Чинний від 1992-01-01] [Електронний ресурс]. – Режим доступу: http://vsegost.com.

85. Іванов Ю.Б. Роль оподаткування в системі інноваційних процесів / Ю.Б. Іванов // Проблеми розвитку податкової політики та оподаткування: монографія. – Харків, ВД «ІНЖЕК», 2007. – С. 88–111.

86. Інформаційне законодавство України [Текст]: наук.-практ. коментар / за ред. Бондаренко С.В. – К.: Юридична думка, 2009.– 241 с.

87. Інформаційне право від Др. Міхаеля Клопфера, Др. Андреаса Нойна // Інформаційне право: стан та перспективи розвитку в Україні: матер. круглого столу. – К., 2004. – 1 квітня. – 63 с.

88. Касьяненко М.М. Організація роботи та управління органами державної податкової служби України: навч. посіб. / Касьяненко М.М., Гринюк М.В., Цимбал П.В. – Ірпінь: Академія ДПС України, 2001. – 229 с. [Електронний ресурс]. – Режим доступу: http://vl-book.ru.

89. Климентьєв О.П. Інформаційна функція української держави: автореф. дис. на здобуття наук. ступеня кандидата юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.П. Климентьєв. – Київ, 2014. – 21 с.

90. Коваль В.Ф. Основні напрями модернізації взаємодії структурних підрозділів ДПС в інформаційній сфері / В.Ф. Коваль, В.І. Теремецький // Вісник Вищої ради юстиції. – 2012. – № 2 (10).– С. 142–157.

91. Копилов В.А. Информационное право: учебник / В.А. Копылов. – 2-е изд., перераб. и доп. – М.: Юристъ, 2003.– 512 с.

92. Копылов В.А. О структуре и составе информационного законодательства / В.А. Копылов // Государство и право. – 1996. – № 6. – С. 99.

93. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра. юрид. наук: спец. 12.00.07 // Кормич Б.А. – Одеса, 2004. – 427 с.

94. Кормич Б.А. Інформаційне право: підр. / Кормич Б.А. – Харків: БУРУН і К, 2011. – 334 с.

95. Косиця О.О. Правове регулювання інформаційного забезпечення адміністративної діяльності у сфері справляння податків: дис. … канд. юрид. наук: 12.00.07 / Косиця О.О. – Ірпінь, 2014. – 232 с.

96. Кохановська О.В. Правове регулювання у сфері інформаційних відносин: монографія / Кохановська О.В. – К.: Національна академія внутрішніх справ України, 2001. – С. 7.

97. Кохановська О.В. Цивільно-правові проблеми інформаційних відносин в Україні: дис. … д-р. юрид. наук: 12.00.03 / Кохановська О.В. – Київ, 2006. – 446 с.

98. Куделя Л.В. Автоматизовані інформаційні системи – інструмент гарантування економічної безпеки підприємства / Л. В. Куделя // Вісник Харківського національного аграрного університету ім. В.В. Докучаєва. – 2013. – № 6. – С. 167–174. – Сер.: Економічні науки.

99. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства / А.М. Кузьменко // Часопис Київського університету права. – 2010. – № 4. – С. 317–321.

100. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України: автореф. дис. на здобуття наук. ступеня кандидата юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Г. М. Линник. – Київ, 2010. – 26 с.

101. Ліпкан В.А. Національна безпека України : навч. посіб. / Ліпкан В.А. – [2-ге вид]. – К. : КНТ, 2009. – 576 с.

102. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції [навч. посібник] / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с.

103. Лопатін С.І. Адміністративно-правові відносини у сфері забезпечення права громадян на інформацію: автореф. дис. на здобуття наук. ступ. канд. юрид. наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / С.І. Лопатін. – Київ, 2010. – 22 с.

104. Лютий І.О. Податки на споживання в економіці України / І.О. Лютий, А. Б. Дрига, М. О. Петренко. – К.: Знання, 2005. – с. 33.

105. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис. на здобуття наукового ступеня канд. юрид. наук: 12.00.01 / Ю.Є. Максименко. – К., 2007. – 22 с.

106. Максимов И. В. Административные наказания / Максимов И.В. – М.: Норма, 2009. – 466 с.

107. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я. Малик, О. Береза // Ефективність державного управління: зб. наук. праць. – 2012. – Вип. 32 – С. 20–27.

108. Мастяниця Й.І. Інформаційні ресурси України: проблеми державного регулювання [Текст]: монографія / Мастяниця Й.І.– К.: НІСД, 2006. – 141 с.

109. Мацюк В.Я. Організаційно-правові засади інформаційного забезпечення управління органами податкової міліції / В.Я. Мацюк // Вісник Запорізького юридичного інституту. – 2003. – № 1. – С. 114 – 123.

110. Монахов В.Н. Государственно-правовые вопросы информационного обслуживания граждан в СССР (Конституционный аспект): дис. … к.ю.н. / Монахов В.Н. – М., 1983. – С. 35–36.

111. Мороз Д.О. Інформаційне забезпечення адміністративно-юрисдикційної діяльності податкової міліції / Д.О. Мороз // Науковий вінник Національного університету ДПС України (економіка, право). – 2011. – № 4 (55). – С. 222–227.

112. Мулявка Д.Г. Організація захисту інформації обмеженого доступу в інформаційних ресурсах ДПС України / Д.Г. Мулявка, Т.О. Рекуненко // Митна справа. – 2012. – № 2 (80). – С. 324–329. – (частина 2, книга 1).

113. Науково-практичний коментар до Податкового кодексу України: в 3 т. / кол. авторів [заг. редакція М.Я Азарова]. – К.: Міністерство фінансів України, Національний університет ДПС України, 2010. – Т. 2. – 506 с.

114. Нестеренко О.В. Засади забезпечення необхідного рівня інформаційної безпеки державної влади / О.В. Нестеренко // Національна безпека: український вимір. – 2009. – № 3 (22). – С. 58–67.

115. Новицька Н.Б. Правове забезпечення інформаційної безпеки / Н.Б. Новицька // Інформаційна безпека людини, суспільства, держави. – 2009. – № 1. – С. 44–47.

116. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: автореф. дис. на здобуття наук. ступеня докт. юрид. наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Олійник. – Київ, 2013. – 34 с.

117. Олійник О.В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів / О.В. Олійник // Право і безпека. – 2014. – № 1 (52) – С. 103–109.

118. Олійник О.В. Правові аспекти оптимізації організаційних засад інформаційної безпеки / О. В. Олійник // Інформаційне право. – 2013. – № 3. – С. 73–78.

119. Партико З.В. Теорія масової інформації та комунікації / Партико З.В.– Львів: Афіша, 2008. – 290 с.

120. Пархоменко В.Д. Наукові і організаційні проблеми управління інформаційними ресурсами [Текст] / В.Д. Пархоменко // Науково-технічна інформація. – 2007. – № 3. – С. 31–36.

121. Перов Д.О. Інформаційні правовідносини в Україні: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Д.О. Перов. – Київ, 2014. – 19 с.

122. Петрик В.М. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 122–134.

123. Петросян В.Г. Проблеми інтегрування інформаційних ресурсів податкової служби України в єдину інформаційну систему правоохоронних органів / В.Г. Петросян // Правова інформатика. – 2010. – №2 (26) – С. 10–16.

124. Письменицький А.А. Фактичний зміст права на інформацію та принцип верховенства права: теоретико-термінологічний аспект / А.А. Письменицький // ПРАВО. – 2009. – № 1 (5). – С. 67–71.

125. Плішкін В.М. Теорія управління органами внутрішніх справ: [підручник] / В.М. Плішкін; за ред. Ю.Ф. Кравченка. – К.: Національна академія внутрішніх справ України,1999. – 702 с.

126. Полушкин А. В. О понятии информационного правонарушения / А. В. Полушкин // Российский юридический журнал. – 2009. – № 3. – С. 208–214.

127. Попова С.М. Інформаційне забезпечення діяльності органів податкової служби / С.М. Попова // Право і безпека. – Харків: ХНУВС, 2011. – № 2 (39). – С. 273–277.

128. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах/ М.М. Присяжнюк, Я.С. Бєлошевич // Вісник Київського національного університету ім. Тараса Шевченка. – 2013. – № 1 (39). – С. 37–40.

129. Рассолов М.М. Информационное право: учеб. пос. / Рассолов М.М. – М.: Юристъ, 1999. – 400 с.

130. Рекуненко Т.О. Адміністративно-правові засади управління інформаційними ресурсами органів державної податкової служби України: дис. … канд. юрид. наук: 12.00.07 / Рекуненко Т.О. – Київ, 2012. – 205 с.

131. Розум О.М. Проблеми виявлення і розкриття комп'ютерних злочинів / О.М. Розум // Організація і практика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку: матер. Всеукр. наук.-практ. конф. (м. Донецьк, 04 грудня 2009 р.). – Донецьк : ДЮІ ЛДУВС, 2009. – С. 164–167.

132. Розум О.М. Впровадження інформаційного забезпечення в діяльність оперативних підрозділів податкової міліції /О.М. Розум // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матер. наук.-практ. конф. (24 грудня 2010 р.). – Львівський державний університет внутрішніх справ. – Львів, 2010. – С. 253–259.

133. Розум О.М. Інформаційне забезпечення виявлення, розкриття та розслідування податкових злочинів / О.М. Розум // Підприємництво, господарство і право. – 2010. – № 10. – С. 177–180.

134. Розум О.М. Особливості інформаційно-аналітичного забезпечення діяльності підрозділів податкової міліції / О.М. Розум // Право та управління. – 2010. – № 1. – С.141–148.

135. Розум О.М. Деякі аспекти інформаційного забезпечення правоохоронної діяльності у сфері оподаткування / О.М. Розум, В.С. Безрученко // Право та управління. – 2011. – № 3. – С. 224 – 229.

136. Росоловський В.М. Автоматизація роботи в органах державної податкової служби: підр. / В.М. Росоловський, В.М. Ріппа; за заг. ред. Росоловського В.М. та Ріппи С.П. – Ірпінь: Академія ДПС України, 2002. – 401 с.

137. Савчишкин Д. Б. Административная ответственность в области связи и информатизации: автореф. дис. на здобуття наук. ступеня канд. юрид. наук / Д. Б. Савчишкин. – М., 2011. – 16 с.

138. Савчишкин Д. Б. Информационно-административное правонарушение: понятие, признаки, состав / Д. Б. Савчишкин // Административное и муниципальное право. – 2011. – № 7 [Электронный вариант]. – Режим доступа : //www.consultant.ru.

139. Семир'янов Д.Я. Інформаційно-аналітичне забезпечення управління підрозділами податкової міліції України: дис. … канд. юрид. наук: 12.00.07 / Семир'янов Д.Я. – Ірпінь, 2004. – 196 с.

140. Сировой О.В. Організаційно-правові засади управління інформаційними ресурсами органів внутрішніх справ України: дис. … канд. юрид. наук: 12.00.07 / Сировой О.В. – Харків, 2006. – 218 с.

141. Системна інформатизація законотворчої та правоохоронної діяльності: монографія / кер. авт. кол. Швець М.Я.; за ред. В.В. Дурдинця та ін. – К.: Навч. книга, 2005. – 639 с.

142. Словарь по кибернетике / под ред. В.С. Михалевича. – [2-е изд.].– К.: гл. ред. УСЭ им. М.П. Бажана, 1989. – 751 с.

143. Снытников А.А. Обеспечение и защита права на информацию / А.А. Снытников, Л.В. Туманова. – М.: Городец-издат, 2001. – С. 101.

144. Стаценко-Сургучова І.С. Організаційно-правові засади інформаційно-аналітичної роботи в органах Державної податкової служби України: дис. … канд. юрид. наук: 12.00.07 / Стаценко-Сургучова І.С. – Ірпінь, 2008. – 200 с.

145. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. – 2011. – Випуск 1 (3). – С. 90–99. – Серія: Економіка, право, політологія, туризм.

146. Стоєцький О.В. Адміністративна відповідальність за правопорушення у сфері інформаційної безпеки України: автореф. дис. на здобуття наукового ступеня кандидат юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / О.В. Стоєцький. – Запоріжжя, 2013. – 19 с.

147. Субіна Т.В. Адміністративно-правове забезпечення інформаційної безпеки в органах державної податкової служби України: дис. ... канд. юрид. наук : 12.00.07 / Субіна Тетяна Володимирівна. – Ірпінь, 2010. – 219 с.

148. Теремецький В.І. Адміністративно-правове регулювання податкових відносин в Україні: дис. ... докт. юрид. наук: 12.00.07 / Теремецький Владислав Іванович. – Харків, 2012. – 219 с.

149. Халфина Р.О. Общее учение о правоотношении / Халфина Р.О. – М.: Юридическая литература, 1974.

150. Хімей В. Основні сучасні проблеми інформаційної безпеки України / В. Хімей // Теле- та радіожурналістика. – 2014. – Випуск 13. – С.127–132.

151. Цехан Д.М. Правове регулювання мережі Інтернет як передумова її декриміналізації / Д.М. Цехан // Актуальні проблеми держави і права. – Випуск 65. Вичитка № 2. – 2012. – С. 668–676.

152. Череповський К.П. Інкорпорація інформаційного законодавства України: автореф. дис. на здобуття наук. ступеня кандидат юридичних наук:12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право»/ К. П. Череповський. – Запоріжжя, 2013. – 19 с.

153. Чуприна О. В. Адміністративна відповідальність за порушення права на інформацію / Чуприна О. В. – К., 2013. – 175 с.

154. Шапка А.В. Інформаційні відносини в податковій сфері: теоретико-правовий аспект / Литвин Н.А., Шапка А.В. // Науковий вісник НУДПСУ (економіка, право). – 2013. – № 4 (63).– С. 54–59.

155. Шапка А.В. Деякі аспекти податкового контролю в умовах розвитку інформаційних технологій / Н.А. Литвин, А.В. Шапка // Реформування податкової системи України в контексті глобалізацій них викликів: матер. наук.-практ. інтернет-конф., ДФСУ, НУДПСУ, Наук.-досл. Центр з проблем оподатк. – Ірпінь, 2014. – С. 150–151.

156. Шапка А.В. Административно-правовое обеспечение информационной безопасности в деятельности фискальных органов / А.В. Шапка // Административное право и процес: история, современность, перспективы развития: тезисы докладов междунар. дистанц. науч.-практ. конф., г. Москва-Запорожье, 21–22 мая 2014 г. – ЗНУ. – 2014. – С. 270–271.

157. Шапка А.В. Адміністративно-правове регулювання інформаційної безпеки в діяльності фіскальних органів / А.В. Шапка // Міліція України: щомісячний інформаційно-популярний та науково-практичний журнал. – 2014. – № 9-10 (207-208).– С. 26–28.

158. Шапка А.В. Склад та особливості інформаційних правовідносин в податковій сфері / А.В. Шапка // Юридичний науковий електронний журнал. – 2014. – № 6.– С. 143–146.

159. Шапка А.В. Понятие информационной безопасности в деятельности Государственной фискальной службы Украины / А.В. Шапка // Право и политика: научно-методический журнал. – 2015. – № 1.– С. 177-181. (периодическое научное издание Кыргызской Республики).

160. Швець М. Інформаційне законодавство України: концептуальні основи формування / Швець М., Калюжний А., Гавловський В., Цимбалюк В. // Право України. – 2001. – № 7. – С. 88.

161. Шевчук О.М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки: автореф. дис. на здобуття наук. ступеня

к. ю. н.: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» // О.М. Шевчук. – Запоріжжя, 2011. – 23 с.

162. Шлома Г.О. Адміністративно-правове забезпечення службової таємниці в органах внутрішніх справ України: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Г. О. Шлома. – Д., 2008. – 20 с.

163. Шпенов Д.Ю. Інформаційні правовідносини: автореф. дис. на здобуття наук. ступеня кандидат юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Д.Ю. Шпенов. – Київ, 2012. – 19 с.

164. Юдін О.К. Інформаційна безпека держави: навч. посіб. / Юдін О.К., Богуш В.М. – Х.: Консум, 2005. – 576 с.

165. Яременко О.І. Інформаційні відносини як предмет правового регулювання: теоретичний аспект / О.І. Яременко // Вісник Хмельницького інституту регіонального управління та права. Науковий часопис. – 2004. – № 1-2 (9-10). – С. 156–161.

166. Ярмакі Х. П.Адміністративно-наглядова діяльність міліції в Україні: дис. … д-ра юрид. наук: 12.00.07 / Ярмакі Х. П. – Х., 2006. – 438 с.

167. Ярочкин В.И. Информационная безопасность: Учеб. пособие для студ. непрофильных вузов / Ярочкин В.И. – М., 2000.

168. Communication from the European Commission: «Network and Information Security: Proposal for a European Policy Approach» (COM (2001) 298 (June 6, 2001) – http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf

169. Council of Europe: http://hub.coe.int/web/coe-portal/navigation/47-countries

170. Developments in the field of information and telecommunications in the context of international security / Report of the Secretary-General.Fifty-six session. 3 July, 2001. United Nations. A/56/164.

171. ENISA Country Reports. 2009. – http://www.epractice.eu/files/media/media2624.pd

172. Estonian Cyber Security Strategy. - http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf

173. EU Seventh Framework Programme (FP7). – http://cordis.europa.eu/fp7/dc/index.cfm

174. The European Network and Information Security Agency (ENISA). – http://www.enisa.europa.eu/

ДОДАТОК А

Проект

**ДЕРЖАВНА ФІСКАЛЬНА СЛУЖБА УКРАЇНИ**

# НАКАЗ

Київ

«__»_____20__р. №_____

Про впровадження «Електронного журналу безпеки»
в ІС «Податковий блок»

Керуючись положеннями ст. ст. 16, 17, 19, 20, 21, 61, 71-74 Податкового кодексу України від 02.12.2010 № 2755-VI, Закону України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI, п. 35 розділу 4 Положення про Державну фіскальну службу України, затвердженого постановою Кабінету Міністрів України від 21 травня 2014 року № 236,

НАКАЗУЮ:

1. Департаменту інформаційних технологій створити програмне забезпечення «Електронний журнал безпеки» в інформаційній системі (далі – ІС) «Податковий блок» для контролю за діями користувачів.

2. Виділити такі характеристики програмного забезпечення «Електронний журнал безпеки» та результати його функціонування:

2.1. Об’єктом програмного забезпечення «Електронний журнал безпеки» є фіксація дій користувачів під час перегляду інформації, яка міститься в ІС «Податковий блок» та її інтегрованій автоматизованій системі «Перегляд результатів співставлення».

2.2. Метою функціонування підсистеми «Електронний журнал безпеки» є зменшення можливості вчинення корупційних дій посадовими особами Державної фіскальної служби під час адміністрування податків, зборів, платежів та здійснення несанкціонованих дій з інформацією.

3. Функції підсистеми «Електронний журнал безпеки»:

3.1. Програмне забезпечення «Електронний журнал безпеки» має фіксувати дії користувачів ІС «Податковий блок» під час формування запиту до системи на вибірку податкових даних суб’єктів господарювання, а також дій під час відкриття та перегляду електронних документів, зокрема: виокремлення безпосередньо запитів у системі (наприклад, за кодом платника); протоколювання звернень до документа в системі (вже за обраним документом).

3.2. Переглядати інформацію щодо зафіксованих дій користувачів в ІС «Податковий блок» можливо лише за допомогою окремої ролі – 420020 «Електронний журнал безпеки», яка призначається для використання лише працівникам підрозділів внутрішньої безпеки.

3.3. За допомогою підсистеми «Електронний журнал безпеки» працівники підрозділів внутрішньої безпеки мають можливість отримувати вихідні дані (документи) стосовно дій в ІС «Податковий блок» та в її інтегрованій автоматизованій системі «Перегляд результатів співставлення» внаслідок формування відомостей під час роботи із зазначеними вище даними, а саме фіксуються: дії користувачів, назва режиму в інформаційній системі, який використовується (можливого ключового фільтру відбору даних), час та дата формування запиту, номера переглянутих електронних документів, ідентифікатор користувача.

3.4. Формування даних у підсистемі «Електронний журнал безпеки» здійснюється лише на центральному рівні функціонування ІС «Податковий блок».

4. Вимоги до накопичення та збереження вихідних даних в ІС «Податковий блок» становить 1,5 – 2 роки (за наявності технічної можливості, але не менше одного року) з можливістю вивантаження у форматі MS Excel.

5. Зміст підсистеми «Електронний журнал безпеки»: програмне забезпечення повинно надавати можливість при перегляді «Електронного журналу безпеки» встановлювати фільтри для вибірки даних за такими окремими показниками:

– реєстраційний номер облікової картки платника податків – користувача ІС «Податковий блок»;

– прізвище, ім’я, по батькові працівника органу ДФС – користувача ІС «Податковий блок»;

– ідентифікатор користувача;

– код органу ДФС;

– назва режиму/підсистеми ІС «Податковий блок»;

– номер електронних даних (електронного документа), які переглядав користувач в ІС «Податковий блок»;

– дата та час дій;

– інформація щодо мережевого підключення (IP-адреси користувача).

6. Необхідна фіксація дій користувачів для забезпечення контролю в таких режимах ІС «Податковий блок»:

– 148 Паспорт, 53 Перевірки, 2000 Податковий аудит;

– 54 Реєстр, 53 Перевірки, 2000 Податковий аудит;

– 57 Журнал податкових повідомлень-рішень, актів з пенею, 53 Перевірки, 2000 Податковий аудит;

– Подана звітність, приймання звітності, 8000 Обробка податкових зобов’язань та платежів (у розрізі реєстраційного номеру документа, поданого платником податку та податкового періоду);

– Перегляд результатів співставлення, Автоматизована система співставлення 9000 Аналітична система (у тому числі обов’язково з побудовою схем руху сум податку на додану вартість у розрізі податкового періоду);

– АІС Скарга Інші системи 9000 Аналітична система;

– АІС Суди Інші системи 9000 Аналітична система (сторони процесу, реєстр судових справ);

– 20 Перегляд та друк інформаційних карток платежів, 19 Ведення інформаційних карток платежів, 7000 Облік платежів;

– 24 Податкові вимоги, 23 Податковий борг, 7000 Облік платежів;

– 196 Суб’єкти фіктивного підприємництва, 189 Моніторинговий центр, 9000 Аналітична система;

– 176 Реєстр суб’єктів фіктивного підприємництва, 5208 Суб’єкти фіктивного підприємництва, 5200 Взяття на облік платника податків, 5000 Реєстрація платника податків;

– Пошук платників податків 5000 Реєстрація платника податків;

– Реєстри платників податків, Ведення окремих реєстрів 5000 Реєстрація платника податків;

– 44 Реєстр підтверджень, 43 Облік податку на додану вартість, 7000 Облік платежів;

– 45 Перегляд журналу висновків, 43 Облік податку на додану вартість, 7000 Облік платежів;

– 314 Перегляд журналу висновків про відшкодування податку на додану вартість, 43 Облік податку на додану вартість, 7000 Облік платежів;

– 225 Відстеження стану непідтверджених сум податку на додану вартість, 43 Облік податку на додану вартість, 7000 Облік платежів;

– 288 Реєстр об’єктів житлової нерухомості, 287 Плата за нерухомість, 7000 Облік платежів;

– 289 Сформовані податкові повідомлення-рішення, 287 Плата за нерухомість, 7000 Облік платежів;

– 405 Перегляд суб’єктів та об’єктів оподаткування, 404 Транспортний податок, 7000 Облік платежів;

– 406 Сформовані податкові повідомлення-рішення, 404 Транспортний податок, 7000 Облік платежів;

– 312 Реєстри платників податків, 5408 Реєстри, 5000 Реєстрація платника податку;

– 507 Реєстр платників акцизного податку з реалізації пального, 5415 Реєстр платників акцизного податку з реалізації пального, 5400 Реєстрація платників окремих податків, 5000 Реєстрація платників податків;

– 5804 Реєстр платників податків на нерухоме майно, відмінне від земельної ділянки, 5801 Облік об’єктів нерухомого майна, 5800 Облік об’єктів оподаткування у вигляді житлової нерухомості платника податків - фізичної особи, 5000 Реєстрація платників податків.

7. Департаменту інформаційних технологій:

7.1. Забезпечити подальший розвиток та безперебійне функціонування підсистеми «Електронний журнал безпеки» в ІС «Податковий блок».

7.2. Негайно інформувати відповідні структурні підрозділи ДФС України у межах їх компетенції про можливі факти несанкціонованого втручання в роботу автоматизованих систем та мереж ДФС України.

8. Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації забезпечити вжиття організаційних заходів та впровадити дієвий механізм захисту підсистеми «Електронний журнал безпеки» в ІС «Податковий блок», а також автоматизованих робочих місць її користувачів від несанкціонованого втручання.

9. Головному управлінню внутрішньої безпеки:

9.1. Забезпечити реалізацію заходів щодо запобігання корупції під час використання посадовими особами ІС «Податковий блок» в апараті ДФС, її територіальних органах за допомогою підсистеми «Електронний журнал безпеки».

9.2. Здійснювати методологічне супроводження складових підсистеми «Електронний журнал безпеки» в межах компетенції структурного підрозділу.

9.3. За фактами виявлених причин і умов вчинення правопорушень під час роботи з ІС «Податковий блок» (несанкціоноване втручання у роботу інформаційної системи, незаконне розголошення інформації тощо) здійснювати підготовку пропозицій правового, соціального, економічного та організаційного характеру, спрямованих на запобігання та припинення таких правопорушень.

10. Департаменту моніторингу доходів та обліково-звітних систем забезпечити внесення цього наказу до Репозиторія звітної і статистичної інформації Державної фіскальної служби України відповідно до наказу ДФС від 07.10.2014 р. № 168.

**Голова**