**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Західноукраїнський національний університет**

**Навчально-науковий інститут публічного управління**

Кафедра фінансів ім. С.І. Юрія

**ПІДГІРЕЦЬ Сергій Олександрович**

**Загрози безпеці інформації органів ДФС України: методи виявлення та шляхи запобігання/ Threats to information security of the SFS of Ukraine: detection methods and ways to prevent**

Спеціальність: 281 – Публічне управління та адміністрування

освітньо-професійна програма – Державна служба

Кваліфікаційна робота

 Виконав студент групи

 ДСПУАзм-25

 С.О.Підгірець

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Науковий керівник:

 д.е.н., професор О.І. Тулай

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ О. П. Кириленко

**ТЕРНОПІЛЬ-2021**

**ЗМІСТ**

Вступ …………………………………………………………………….…….4

Розділ 1. Теоретичні та організаційно-правові засади гарантування безпеки інформації…………………………………………………………….……9

* 1. Сутність, роль та значення безпеки інформації державних органів………………………………………………………………………………...8
	2. Нормативно-правове регулювання безпеки інформації……….….13

Висновки до розділу 1………………………………………………………20

Розділ 2. Сучасні методи виявлення загроз безпеці інформації органів ДФС України………………………………………………………………………..22

2.1. Класифікація потенційних загроз безпеці інформації……………….22

2.2. Моніторинг каналів витоку інформації ……………………………..35

2.3. Практичні аспекти застосування методів виявлення загроз інформації …………………………………………………………………41

Висновки до розділу 2 ……………………………………………………..44

Розділ 3. Шляхи запобігання загрозі безпеки інформації органів ДФС України……………………………………………………………………….……46

3.1. Напрямки вдосконалення інформаційної діяльності та методів її захисту………………………………………………………………………………46

3.2. Розробка алгоритму дослідження стану забезпечення безпеки інформації у контексті новітніх тенденцій………………………………………63

Висновки до розділу 3 ……………………………..………………………73

Висновки та пропозиції………………..……………………………………75

Список використаних джерел………………………………………………80

**Вступ**

У світові спостерігатиметься загальне зростання напруження, насамперед, – в основних сферах життєдіяльності людства – економічній, фінансовій, енергетичній, торговій, технологічній, й безпековій.

Гібридна воєнна агресія, вкрай нестабільне становище у світі (загострення конфліктів, поява нових осередків напруження) та, як результат, суттєве погіршення безпеки у міжнародному середовища разом при значному зменшенні ролі інстанцій міждержавних утворень та організацій у розв’язанні воєнних конфліктів дають чітке розуміння того, що безпека кожної держави не може гарантуватися ззовні.

В умовах викликів і загроз національній безпеці в контексті розвитку інформаційного суспільства та сучасних цифрових трансформацій, здійснюється розбудова та реалізації політики держави у галузі інформаційної безпеки, формування системи стратегічних комунікацій сектору безпеки і оборони, розвиток національного законодавства у цій сфері та інших актуальних питань інформаційної безпеки людини, суспільства і держави.

Разом з цим, в умовах модернізації органів державного управління на тлі наближення у всіх сферах до стандартів Європейського Союзу відбувається стрімкий розвиток інформаційно-телекомунікаційного забезпечення функціонування органів державного управління.

Сучасні інформаційні системи та комп’ютерні технології відіграють одну з провідних ролей у вирішенні завдань підвищення ефективності всіх виробничих процесів в цілому. Це має як позитивні, так й негативні наслідки. З одного боку, використання можливостей в правовому полі вищезазначених технологій надає можливість кожній людини, суспільству в цілому та державному апарату краще задовольняти власні інтереси та реалізовувати покладені на них завдання. З іншого, – використання нових технічних можливостей у протизаконних цілях сприяє зловмисникам учиняти злочини, незважаючи на відстань, розташування, місцезнаходження тощо.

Забезпечення безпеки інформаційної діяльності, безпосередньо інформаційних ресурсів установи, а також всіх інших ресурсів є одним із пріоритетних завдань для сучасного державного органу, діяльність якого пов’язана безпосередньо з використанням в роботі інформації, розголошення або втрата якої може завдати шкоди як державним інтересам так й інтересам окремих її громадян. Існування конкурентної інформаційного середовища, тобто середовища в якій проводяться з боку потенційних зловмисників (злочинців) противоправні дії, метою яких є мінімізація або запобігання притягнення до відповідальності за скоєні злочини у сфері оподаткування, спонукає до організації комплексного захисту інформації.

При цьому під комплексним захистом мається на увазі рішення двоєдиного завдання:

* виявлення можливостей несанкціонованого впливу зловмисників на інформаційні ресурси установи для ознайомлення, спотворення, знищення, поширення інформації тощо,
* запобігання, тобто усунення вказаних вище можливостей для усунення негативних наслідків при реалізації завдань та функцій, які покладені на органи ДФС України.

Тема документообігу у державних установах, в яких існує сувора регламентація використання інформації, особливо інформації з обмеженим доступом, не достатньо досліджена на сьогодні в Україні. відсутні наукові праці, в яких здійснюються дослідження проблем безпеки інформації. В наукових дослідженнях з питань захисту інформації здебільшого містяться результати аналізу нормативно-правової бази, яка регулюють обіг інформації, розкриваються суто технічні аспекти проблеми або ж досліджуються фізичні процеси виникнення або штучного створення каналів витоку інформації тощо. Окремі питання щодо захисту інформації розкриваються у наукових роботах В. Алещенка, А. Амоши, В. Бережинського, А. Вітченко, В. Возженикова, В. Галєева, Г. Губерної, В. Гошовської, А. Коровникова, С. Корольова, Е. Лібанової, В. Скуратівського, Н. Чалдимова та А. Шишканова та інших.

Віддаючи належне теоретичній і практичній значущості наукового доробку зазначених учених, слід звернути увагу на те, що проблема модернізації систем управління інформаційною системою у діяльності органів державної влади (установ) недостатньо глибоко досліджена у вітчизняній наукові літературі та потребує подальшого вивчення.

**Метою** кваліфікаційної роботи є науково-теоретичне обґрунтування та напрацювання рекомендацій щодо покращення системи забезпечення функціонування безпеки інформації в органах ДФС Україні.

У відповідності до мети у кваліфікаційної роботі сформульовані наступні завдання дослідження:

* дослідити зміст, роль та значення структури та організацію функціонування системи захисту інформації в органах ДФС Україні;
* обґрунтувати теоретичні та організаційно-правові засади побудови системи захисту інформації в органах ДФС Україні;
* проаналізувати сучасний стан та проблеми у сфері;
* узагальнити вітчизняний досвід реалізації системи захисту інформації;
* запропонувати шляхи удосконалення захисту інформації в органах ДФС Україні.

**Об’єктом**дослідження є інформаційна діяльність органів ДФС України

**Предметом** дослідження виступають теоретико-методологічні та практичні аспекти запобігання порушення безпеки інформації, яка використовується для вирішення завдань та функцій у процесі діяльності ДФС України.

**Методи дослідження**. Основним методом упроцесі дослідження використовується діалектико-системний підхід, у відповідності до якого процеси та явища вивчаються у взаємозалежності, взаємозв’язку та динаміці. Завдання в роботі під час дослідження втілювалися шляхом комплексного запровадження загальнонаукових та спеціальних методів: логічного, етимологічного, порівняння, аналізу і синтезу, узагальнення, статистичного, аналогії.

В якості теоретичної та методологічної бази для проведення дослідження використовували нормативно-правові акти зарубіжжя та України, довідкові матеріали, монографії, матеріали науково-методичних і науково-практичних конференцій, дослідження фахівців щодо розкриття різних аспектів з даної проблематики.

**Інформаційну базу**складають наукові дослідження українських та закордонних науковців, звітні дані Державної фіскальної служби України, Державної служби статистики України, Служби безпеки України, Міністерства фінансів України.

**Наукова новизна одержаних результатів.** Елементи наукової новизни, за результатами дослідження, зводяться до наступного:

* здійснено комплексний аналіз організаційно-правових засад та практики забезпечення безпеки інформації в органах ДФС Україні;
* оцінено сучасний стан безпеки інформації, на основі чого запропоновано низку практичних заходів для усунення виявлених недоліків;
* запропоновано напрями удосконалення вітчизняної системи захисту інформації в органах ДФС Україні з урахуванням практичного досвіду.

**Практичне значення одержаних результатів.** Робота справляє позитивний вплив щодо вдосконалення методів дослідження інформаційного середовища установи з метою виявлення можливих ризиків для інформаційних баз та підвищення ефективності роботи підрозділів установи в частині здійснення контролю за станом безпеки інформації

**Структура й обсяг роботи.** Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи складає 86 сторінок. У роботі наведено 5 таблиці та 12 рисунків. Список використаних джерел налічує 58 позицій.

 У першому розділі розкриваються теоретичні та організаційно-правові засади забезпечення безпеки інформаційної діяльності в структурі загальної діяльності установи в цілому.

 Другий розділ присвячений аналізу практики та проблематики здійснення захисту інформації в держаних установах, в тому числі в органах ДФС Україні.

 У третьому розділі висвітлюються напрями удосконалення системи інформаційної безпеки та сучасні тенденції розвитку у світлі сучасних інформаційних технологій.

**Розділ 1**

**Теоретичні та організаційно-правові засади**

**гарантування безпеки інформації**

* 1. **Сутність, роль та значення безпеки інформації державних органів**

Термін «інформація»  походить від латинського іnformatіo і перекладається буквально: ознайомлення, роз’яснення, уявлення, поняття. Можна обмежитись даним визначенням терміну «інформація»  оскільки в більшості наукових праць з проблем інформаційної безпеки, поняття «інформація»  взагалі не визначається. З іншого боку, аналіз наукової літератури свідчить про наявність безлічі визначень сутності інформації, серед яких можливо наголосити на чотирьох принципових підходах.

Так, академік В. Глушков вважає, що інформація є атрибутом (невід’ємною властивістю) усіх матеріальних тіл, а не тільки розумних живих істот. Інформація у неорганічній природі існує об’єктивно, але ніби в потенційній формі [9]. З появою живої природи (організмів), інформація починається використання для пізнання й управління. Отже, інформація існує в просторі й часі споконвічно, як властивість матерії і руху. Засновник кібернетики Н. Вінер стверджував, що інформація є властивістю лише високоорганізованої, тобто живої матерії. На його думку, інформація й інформаційні процеси властиві тільки біологічній і соціальній формам руху матерії. Він вважав, що всі живі істоти розвиваються завдяки постійному обміну інформацією з оточуючим середовищем, взаємодії із природою, [5]. Розгляд інформації за соціальним підходом пропонує В. Афанасьєв. Він розуміє інформацію як результат діяльності саме тільки матерії соціальних форм (суспільства). Інформація може існувати незалежно ні від кого в просторі, часі, але її прояв відбувається лише при пізнанні навколишнього світу людиною [3]. Таким чином, інформації належить інтегруюча роль, завдяки якій людина, адаптується до соціальних умов. Загалом, з огляду на зазначене, інформація є підґрунтям процесів саморегулювання у живій природі.

Водночас К. Шеннон пропонує функціональний підхід до розуміння сутності інформації, та вважати її властивістю систем, які самоорганізуються, й у живій природі й у техніці [58]. До них, наприклад, відносять живі істоти й кібернетичні системи, для яких характерні процеси саморегулювання завдяки обробці інформації. На наш погляд, найбільш узагальненим є тлумачення досліджуваного поняття у Законі України «Про інформацію», відповідно до якого «інформація – це будь-які відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [38].

Разом з цим, виходячи із наукових підходів і законодавчих актів України, необхідно також визначити інформацію як відомості, які задокументовані, публічно оголошені щодо подій, явищ, що відбуваються. Інформація є важливим джерелом влади та базовою передумовою життєздатності соціальних систем. Інформація у будь-якій установі (державному органі) є підґрунтям (основою) діяльності та реалізації її основних завдань та функцій, без обміну інформаційними потоками у системі державного управління виникне колапс.

Таким чином, інформаційна складова є визначальною щодо відображення зав’язків у системах соціального порядку, системний аналіз яких має бути підґрунтям у вирішені проблем безпеки особи (індивіда), соціальних утворень. Отже, вищеописане дає підстави розглядати «інформацію» як одну з найважливіших складових існування та розвитку суспільства, країни, її державних інституцій.

Існує загально прийняте визначення безпеки — це відсутність загроз життєво важливим інтересам людини, як то: її життю, здоров’ю і добробуту. Безпека належить до базових потреб і є потребою дефіциту, що означає: доки людина не почувається безпечно, вона не може дбати про потреби вищого порядку — соціальні, духовні. За аналогією все вищевказане можливо віднести до будь-якого утворення, в тому числі й державного органу.

За відсутності безпеки у будь-якій галузі, в тому числі і в інформаційній усі зусилля по реалізації державних функцій органом публічної політики можуть зведені нанівець. При цьому необхідно розрізняти поняття «інформаційна безпека» та «безпека інформації». Щодо першого поняття, увага акцентується власне на інформації, а у другому випадку – на безпеці. Так, Б. Кормич трактує безпеку інформації як стан захищеності норм, критеріїв, інформаційних процесів, якій створює умови існування людини, держави та суспільства. як суб’єктів цих процесів та відносин які встановлених [13]. Аналізуючи поняття «безпека інформації» необхідно звернути увагу на її поліаспектність. По-перше, безпека інформації – це стан інформації, інформаційних ресурсів та інформаційно-телекомунікаційних систем, при якому з необхідною вірогідністю забезпечується захист інформації. По-друге – це стан захищеності інформації, що обробляється засобами обчислювальної техніки або автоматизованої системи від внутрішніх та зовнішніх загроз*.*

За моделлю СІА при вирішенні питань безпеки інформації найчистіше прийнято застосовувати основних властивостей інформації:

* конфіденційність — параметр інформації, при наявності якого інформація не може бути отримана користувачем, якій неавторизований.
* цілісність — означає неможливість модифікації неавторизованим користувачем.
* доступність — параметр інформації, при наявності якого до інформації отримує доступ користувач при наявності відповідних повноважень [58].

Саме стан забезпечення незмінності для власника цих характеристик інформаційних ресурсів слід розглядати, як безпеку інформації. Розглянемо інформаційну складову на загальнодержавному рівні у системі національної безпеки держави. Національні інтереси, як підґрунтя формування національної безпеки, є збалансування інтереси громадян, суспільства і держави у сферах їх життєдіяльності. При цьому гарантується збереження загальнонаціональних цінностей, суверенітет держави і її територіальна цілісність, розвиток суспільства та економіки. Головним елементом політичної системи є держава, яка покликана найточніше виражати національні інтереси, вирішувати соціальні протиріччя та забезпечувати права людини. Одним з багатьох означень системи державних органів можливо назвати «спеціальний апарат управління». Державний орган - певна державна інстанція, яка виступає від імені держави, засновується та утворюється державою, в установленому порядку та діє за її уповноваженням. Державні органи в системі національної безпеки покликані цілеспрямовано відстоювати у повсякденній діяльності національні інтереси. Необхідно зазначити, що система забезпечення національної безпеки має за мету запобігання реальних та потенційних загроз, які унеможливлюють чи ускладнюють реалізацію національних інтересів, в тому числі й загрозам на безпеку інформаційних ресурсів держави.

Як вже зазначалось, що інформаційна безпека є складовою національної безпеки, а саме – захищеність в тому числі суспільства і держави в сфері інформації (інформаційна і телекомунікаційна інфраструктура, інформація та її параметри). Але інформаційна безпека має особливістю те, що, як невід’ємна частина, вона входить до інших сфер національної безпеки: економічної, воєнної, політичної безпеки тощо. На сучасному етапі для національної безпеки України в низці інших є таки основні загрозами в сфері інформаційної діяльності, а саме: розголошення секретної інформації, а також іншої конфіденційної, що є власністю держави. Забезпечення безпеки інформації є обов’язковою умовою, завдяки якої можуть бути втілені інші складові національної безпеки, адже всі типи взаємодій між суб’єктами суспільства в інформаційній сфері ґрунтуються на обігу інформації. При цьому в першу чергу в системі органів державної влади використовуються інформаційні ресурси. Ці бази інформації постійно перебувають під загрозою небезпек з боку зловмисників. Природно що рівень забезпечення безпеки інформації в окремих державних органах напряму впливає на загальний рівень інформаційної безпеки суспільства й держави в цілому. Саме тому захист інформаційних ресурсів в окремому державному органі щодо збереження їх властивостей є необхідною запорукою забезпечення національної безпеки країни в цілому. При цьому забезпечення інформаційної безпеки має здійснюватись з дотриманням таких принципів, як законність, баланс інтересів між особою, суспільство і державою; комплексність; системність; поєднання з міжнародними системами безпеки.

* 1. **Нормативно-правове регулювання безпеки інформації**

В умовах гібридної агресії Росії, посилення загроз, і в цілому зростання нестабільності у світі як наслідок поширення недостовірної, упередженої інформації виникають загрози в інформаційній галузі. Закон України «Про основи національної безпеки України» встановлює однією із реальних та потенційних загроз національній безпеці в інформаційній сфері є розголошення інформації з обмеженим доступом, зокрема інформації, яка становить державну таємницю, або іншої інформації щодо забезпечення захисту національних інтересів суспільства і держави [39].

Інформаційна безпека має декілька напрямків її забезпечення (рис 1.1).

Напрямки щодо забезпечення інформаційної безпеки

правовий

програмно-технічний

організаційний

морально-етичний

Рис. 1.1. Напрямки забезпечення інформаційної безпеки.

*Джерело*: складено автором на основі наукових публікацій [36].

Природно, що правові аспекти інформаційної безпеки в сучасних умовах набули нової уваги з боку фахівців. Взаємозалежність права та інформації показує, що право продовжує мати основне своє призначення щодо визначення відносин у процесах інформаційного забезпечення всіх інших соціальних відносин. Правовою основою гарантування безпеки інформації є сукупність різних юридичних норм, що відображають сутність процесів, які відбуваються в інформаційній сфері щодо забезпечення безпеки, утворюючи єдину систему, яка спрямована на підтримання збалансування інтересів між особою, держави та суспільства у сфері обігу інформації.

У Конституції України (ст.ст. 17, 19, 31, 32, 34, 50, 57, 64) визначені основні засади інформаційної безпеки держави [12]. Підґрунтя інформаційної діяльності та закріплення права громадян України на інформацію здійснюється Законом України «Про інформацію» [38]. Закон встановлює правові основи обігу (одержання, використання, поширення та зберігання) інформації, напрямки державної інформаційної політики, визначає суб’єкти та об’єкти учасників інформаційних відносин, доступ до інформації та забезпечення її охорону. Інформація обумовлюється як відомості (дані), які можуть зберігатись за допомогою матеріальних носіїв, в електронному вигляді, а захист її – низька заходів правового, адміністративного, організаційного, технічного характеру, які забезпечують необхідні для власника властивості: цілісність та належний порядок доступу до неї (Закон України «Про інформацію» ст.1).

Законом України «Про Концепцію Національної програми інформатизації» інформаційна безпека розглядається як частина національної безпеки, її політичної, економічної, оборонної та інших складових [40]*.* У Законі України «Про основи національної безпеки України» [41] поняття «інформаційна безпека» не розкривається, а увага фокусується на інформаційній сфері національної безпеки. При цьому, не подається визначення цього поняття, а лише перераховуються загрози та напрями державної політики у цій сфері.

З метою захисту інтересів держави у 2013 р. Кабінетом Міністрів України прийнято Стратегію розвитку інформаційного суспільства в Україні [42]згідно з якою інформаційна безпека віднесена до сфери розвитку інформаційного суспільства. Також необхідно наголосити, що з появою нових загроз безпеці внаслідок агресії Російської Федерації прийнято Стратегію сталого розвитку «Україна-2020» [43],у якій окреслюються вектори реформування національної безпеки; Стратегію національної безпеки України [44] та Стратегію кібербезпеки України [45], уяких значну увагу приділено питанням інформаційної безпеки.

Організаційно-правове забезпечення безпеки інформації охоплює процеси розробки; реалізації та саморегулювання. Тобто це науково обґрунтована система правових й інших засобів, за допомогою яких держава та громадянське суспільство здійснює вплив на інформаційні відносини (реалізація інформаційної безпеки, саморегулювання) і відносини, враховуючі черговість завдань і цілей, які виникають перед суспільством.

У зв’язку з розвитком інтеграційних процесів, входженням України в європейський інформаційний простір, інформаційною агресією Російської Федерації пріоритетне значення набувають міжнародно-правові акти. Адже реалії інформаційної війни встановлює нові правила взаємодії. Вітчизняне законодавство, адміністративні правила, техніка та практика державного регулювання інформаційної безпеки повинні бути виведені на рівень стандартів Організації Північноатлантичного договору НАТО і Європейського Союзу з урахуванням національних особливостей інформаційної інфраструктури.

Рішенням Ради національної безпеки і оборони України (введеного в дію Указом Президента України № 449/2014 від 01.05.2014), одними із пріоритетних завдань для уповноважених за компетенцією органів державної влади є розвиток національного законодавства з метою приведення його до міжнародних стандартів у питаннях інформаційної і кібернетичної безпеки, розвиток державної політики у галузі інформаційної безпеки країни, створення спеціальних програмних і технічних систем захисту інформаційних баз держави та телекомунікаційних мереж, тощо [46].

«Публічна інформація» як термін визначено у Законі України «Про доступ до публічної інформації». Даним Законом зафіксовано, що публічна інформація є відкритою. Окремо законом встановлені випадки при яких припиняє бути відкритою. Перелік цих випадків вичерпний. Таким чином передбачається існування публічної інформації з обмеженим доступом, яка поділяється на інформацію конфіденційну, таємну та службову.

Розглянемо більш детально обмеження доступу до інформації згідно до діючого законодавства. При цьому має відбуватись дотримання вимог щодо: інтересів національної безпеки, громадського порядку, територіальної цілісності, охорони здоров'я, захисту інтересів, прав та репутації інших людей, з метою не допущення розголошенню інформації, яка одержана конфіденційно та т.ін.

Здійснюючі аналіз історії захисту та охорони державної таємниці необхідно прийти до висновку, що для України, як і для інших держав, що утворилися в пострадянському просторі, питання захисту інформації регламентувалися для загалу закритими підзаконними нормативними актами, тобто питання охорони державної таємниці від суспільства відчужувалися [20]. Систему організації охорони державної таємниці, структуру та фінансування її функціонування не розглядалися та не обговорювалися публічно у принципі, рівно як й механізм, і методи, їх ефективність і дієвість.

Сьогодні формування державно-правової сфери базується на основних засадах Конституції України і реалізується за допомогою Законів Верховною Радою України, указів Президента України, рішень Ради національної безпеки і оборони України, постанов Кабінету Міністрів України, наказів Служби безпеки України, Державної служби спеціального зв’язку та захисту інформації України та інших нормативно-правових документів, якими регулюється ця сфера суспільних відносин. Розроблено і введено в дію ряд загальнодержавних, відомчих нормативно-правових актів, що в цілому дозволило створити систему для забезпечення стану сфери охорони державної таємниці та її функціонування, як одну з складових забезпечення національної безпеки з метою недопущення нанесення шкоди у разі розголошення відомостей, що не підлягають розголошенню та охороняються державою, становлять державну таємницю.

Разом з цим, необхідно наголосити на визначенні законодавством питань поділу різних видів інформації, яка циркулює в тому числі й в державних установах, адже в подальшому це суттєво впливає на визначення окремих напрямків політики безпеки інформації в установі. Кожному громадянину забезпечується вільний доступ до інформації щодо нього, крім випадків, передбачених законами України. У розділі ІІІ Закону України «Про інформацію» наведений порядок надання доступу до різного типу інформації. За режимом надання доступу до інформації розрівняється на відкриту інформацію а також інформацію що до якої доступ є обмеженим. Контроль за режимом доступу до інформації здійснює держава. Безпосередньо контроль покладається на спеціальні органи,

Інформація

Відкрита інформація

Таємна інформація

Службова таємниця

Державна таємниця:

таємно

цілком таємно

особливої важливості

Інформація з обмеженим доступом

Конфіденційна інформація

Для службового користування

Не для друку

Таємниця слідства і дізнання

Професійна таємниця

Банківська таємниця

Таємниця нарадчої кімнати

Таємниця псевдоніму

Таємниця нотаріальних дій

Комерційна таємниця

Таємниця страхування

Адвокатська таємниця

Таємниця усиновлення

Лікарська таємниця

Таємниця листування, телефонних розмов та телеграфних відправлень

Рис. 1.2. Класифікація інформації відповідно до Закону України «Про інформацію»

*Джерело:* Складено автором на основі Закону України «Про інформацію» [38].

які визначаються Верховною Радою України і Кабінетом Міністрів України. За правовим режимом в свою чергу інформація щодо якої доступ обмежений поділяється на секретну та конфіденційну.

Інформація, яка за своїм статусом визначена як конфіденційна законодавство визначається як відомості, якими володіють фізичні чи юридичні особи. Вони мають право поширювати її за їх бажанням та на передбачених ними умовах. Громадяни, юридичні особи, які володіють інформацією різного характеру, яка отримана власним коштом, або такою, яка є предметом їх інтересу і не порушує визначеної законом таємниці, можуть самостійно визначати режим доступу до неї. Виняток становить інформація, правовий режим якої встановлено органами державної влади (Верховною Радою України за поданням Кабінету Міністрів України) (економічної та фінансової сфер), та інформація, втаємничення якої являє становить загрозу життю, здоров’ю людей.

До секретна інформації є інформація, яка містить дання, які становлять державну або іншу згідно законодавства таємницю, розголошення (оприлюднення) якої може завдає шкоди особі, суспільству та державі. Визначеними законами органами держави встановлюється порядок користування таємною інформацією, що не становить державної таємниці, та захист її за умов додержання вимог Закону України “Про інформацію”. Без згоди її власника така категорія інформації може бути поширена, якщо вона є суспільно значимою, тобто є предметом зацікавленості громадськості при умові наявності переваги знати цю інформацію громадськістю над правом її власника на захист.

Державна таємниця є особливим типом таємної інформації. До неї належить інформація щодо оборони, зовнішніх відносин, економіки, безпеки держави та правопорядку, несанкціонований витік якої може завдати шкоди державі і які встановлюється згідно вимог законів, та підлягає охороні державою. Законом України “Про державну таємницю” регламентується порядок встановлення інформації до відомостей, що є державною таємницею, порядок її обігу та захисту, доступ до неї, а також визначено законодавчу основу розбудови системи охорони державної таємниці в Україні [47]. Закон передбачає визначення ступені секретності інформації шляхом надання грифів: "Таємно", "Цілком таємно" та "Особливої важливості".

Серед загроз національній безпеці в інформаційній сфері Концепцією національної безпеки України у розділі ІІІ «Загрози національній безпеці України» окремо виділено поняття «витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави» [48].

Подальша інформатизація суспільства викликала необхідність прийняття нормативної бази у сфері застосування новітніх інформаційних технологій, а саме: Закони України «Про телекомунікації, «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію», [Постанови Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373](https://zakon.rada.gov.ua/laws/show/373-2006-%EF%BF%BD), а у Кримінальний кодекс України було введено розділ XVІ, в якому визначалася відповідальність за злочини в інформаційній сфері. Однім з важливих напрямків забезпечення інформаційної безпеки в сучасних умовах є технічний захист інформації. Держава політику України у цієї сфері визначається прийнятими законами та підзаконними актами на виконання Концепції технічного захисту інформації в Україні [49] та подальший розвиток системи захисту інформації в Україні. Підґрунтя було закладено у 1994 році затвердженням Постанови Кабінету Міністрів України «Про затвердження Положення про технічного захисту інформації в Україні»[50].

Указ Президента України 1999 року «Про Положення про технічного захисту інформації в Україні» № 1229 від 27.09.1999 надав новий імпульс в галузі, визначив суб’єкти системи технічного захисту інформації, завдання органів, щодо яких здійснюється такий захист. Положеннями Концепції технічного захисту інформації в Україні визначено напрямки державної політики у галузі захисту інформації інженерно-технічними заходами. Зокрема визначено: технічного захисту інформації – складова частина втілення заходів інженерно-технічного характеру щодо доступу, цілісності та доступності баз інформації, яка є державною та іншою таємницею, конфіденційної інформації.

Поняття у відповідності до положень Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» технічний захист інформації визначається як вид захисту інформації, який має за мету втілення інженерно-технічними заходами, програмними і технічними засобами унеможливлення розголошення, руйнування та блокування інформації, порушення доступу до інформації та її цілісності [51]. Необхідність розвитку технічного захисту інформації обумовлено зростанням загроз для інформації, які виникають у наслідок лібералізації відносин суспільних та міждержавних, кризовими станами в економіці, застосуванням обчислювальної техніки та технічних засобів зарубіжного виробництва, розповсюдження засобів несанкціонованого доступу та впливу на інформацію.

Зі створенням організаційних та правових основ технічного захисту інформації одночасно були започатковані правові та організаційні основи криптографічного захисту інформації. Положення про порядок здійснення криптографічного захисту інформації в Україні було прийнято Указом Президента України у травні 1998 року. Закон України «Про Національну систему конфіденційного зв'язку» був прийнятий у липні 2002 року, у січні 2003 року видано розпорядження Президента України **«**Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку».

**Висновки до розділу 1**

За результати проведеного дослідження теоретичних та організаційно-правових засад гарантування безпеки інформації ми дійшли наступних висновків, що в сучасний період відбувалось формування правових та організаційних основ інформаційної безпеки. Прийняті закони та підзаконні акти за нормами та положеннями, основними принципами, відповідають міжнародним конвенціям з прав людини та міжнародно-правовим стандартам.

Сталий розвиток сфери інформаційно безпеки державного будівництва вимагатиме удосконалення існуючої інфраструктури захисту інформаційних ресурсів, законодавчих і підзаконних актів, нормативних документів, якими встановлюється порядок діяльність інфраструктури, а також діяльність системи органів державного управління, установ, організацій в науковій та виробничій сферах, які мають в обігу інформацію з обмеженим доступом.

Разом з тим необхідно пам’ятати, що постійний розвиток науки та технологій тягне удосконалення технічних засобів та способів несанкціонованого здобуття (зняття) інформації та засоби протидії цим протиправним діям. Зважаючи на постійну боротьбу у інформаційній сфері, що є один з важливих складових сучасної світової політики, для гарантування державної незалежності Україні необхідно і в подальшому удосконалювати та розвивати правові засади інформаційної безпеки.

**Розділ 2**

**Сучасні методи виявлення загроз безпеці інформації органів ДФС України**

**2.1. Класифікація потенційних загроз безпеці інформації**

З метою характеристики інформаційного середовища органу Державної фіскальної служби України, на наш погляд, необхідно окремо докладніші розкрити види інформаційних ресурсів, які перебувають в обігу, у зв’язку з реалізацією цією установою державних завдань. Відповідно спробуємо розглянути та провести класифікацію інформації, яка використовується в установи. При цьому, необхідно підкреслити, що в державній установі захисту підлягає вся інформація, що перебуває в обігу, але в даному випадку, досліджуємо тільки інформацію з обмеженим доступом.

Інформація розрізняється по формах представлення (фізичне середовище) та видах матеріальних носіїв. З точки зору її захисту, інформацію найзручніше поділити на:

* документальну на матеріальних носіях;
* акустична (мовна);
* інформація, що обробляється технічними засобами (комп’ютерна, копіювальна, засоби передачі тощо).

Документальна інформація - це передбачена законом матеріальна форма отримання, зберігання і поширення інформації шляхом фіксації її в графічному або літерно-цифровому вигляді на папері, магнітній, кіно-, відео-, фотоплівці або на іншому матеріальному носії. Мовна інформація виникає під час проведення в приміщенні розмов, при роботі систем звукопідсилення та звуковідтворення.

При вирішені питань запобігання витоку інформації з усіх її властивостей прийнято виділяти деякі з них. Ці властивості можна розглядати бажаними станами інформації (носіїв інформації) для власника або користувача інформації, а саме як зазначалось раніше це: цілісність, конфіденційність, доступність. Таким чином, вся діяльність щодо захисту інформації здійснюється з метою збереження цих властивостей інформації.

Загроза інформаційній безпеці — сукупність умов і факторів, що створюють небезпеку її встановленого рівня. Події, які можуть порушити один з зазначених параметрів, відповідно, прийнято називають, як загрози порушення: цілісність, конфіденційність, доступність [6].

Розглянемо більш докладніше існуючі небезпеки для потрібних нам властивостей інформації. Розголошення інформації з обмеженим доступом є метою загрози порушення обмеження доступу (конфіденційності). Загрози конфіденційності реалізуються для подолання заборон режиму переміщення відомостей від джерела до одержувача. Конфіденційність інформація зберігається при додержанні насамперед режимної адекватності носіїв інформації (відповідність режимів доступу носіїв інформації (а саме: джерела та одержувача) під час їх взаємодії. Лише при переміщенні інформації можливе порушення інформаційної безпеки. Як приклад: несанкціоноване ознайомлення (читання) документа з паперового носія відбувається шляхом перенесення (копіювання) інформації в мозок людини, яка стає одержувачем (носієм) цієї інформації. Під час передачі інформації можлива заміна її носія. Як приклад, носіями відомостями при її передачі можуть бути: середовища матеріального характеру (оточуючі конструкції, повітря, метал та ін.), датчики, сенсори та інші перетворювачі (інші об’єкти живої й неживої природи, що виконують роль проміжних носіїв інформації).

Загрози для реалізації порушення доступності спрямовані на створення ситуацій, при який інформаційні ресурси стають недоступними або знижується ( як приклад працездатність обчислювальної системи). Загрози для реалізації порушення цілісності характеризується у спотворенні або зміні неавторизованою особою інформації, що перебуває в обігу (зберігається, обробляється, передається). Цілісність інформації може бути порушена сумісно, а також унаслідок об’єктивного впливу з боку середовища, що оточує носій інформації.

Одже, якщо є важлива інформація, то безперечно ж, є вірогідність дій, які можуть заподіяти шкоду цій інформації. Усі такі дії можуть бути здійснені тільки при існуванні будь-яких можливостей. А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виникати. Таким чином можна вибудовується послідовність дій та наслідків, а саме: джерело загрози – фактор (вразливість) – загроза (дія) – наслідки (атака) [11].

Пропоную розглянути поділ загроз безпеці інформації при різних підходах. Загрози можуть виникати й усередині організації – внутрішні джерела, і зовні, і створюються джерелами загроз. В свою чергу вони поділяються на три види, які обумовлені:

- діями суб’єкта (антропогенні);

- технічними засобами (техногенні);

- стихійними джерелами.

Зупинимось докладно на визначені джерел загроз та визначимо їх. Антропогенного характеру є суб’єкти, які можуть скоювати дії злочинного характеру (навмисні або ні). Тільки при цьому можливо розглядати виникнення збитків. Ця група найчисельніша та цікава для вивчення в наслідок прогнозованості її суб’єкта та можливості запровадження запобіжних заходів. Антропогенне джерело характеризується наявністю у суб’єкта доступу (санкціонованого або несанкціонованого) до штатних засобів захищає мого об’єкта.

Відповідно ці суб’єкти (джерела небезпеки) поділяються на зовнішні та внутрішні. Джерела, які відносяться до зовнішніх, є випадкові та навмисні та мають різний рівень кваліфікації. Внутрішніми суб’єктами, як правило, виявляються висококваліфіковані спеціалісти з програмування та технічного обладнання, які обізнані з завданнями, структурою, функціями та принципами роботи установи, системи захисту інформації, використовують обладнання та технічних засоби організації. Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел є особи з відхиленнями у психіці, завербовані агенти, які можуть бути з числа основного, допоміжного та технічного персоналу, а також представників служби захисту інформації.

Друга група є джерела загроз, що обумовлена технократичним розвитком цивілізації, наслідки якого, вийшли з-під контролю людини та діють самі по собі. Людство все більше залежне від техніки, і загрози, які виникають при застосуванні техніки, менш можливо прогнозувати, потребують більшої уваги та можуть бути особливо небезпечними. Технічні засоби, що є джерелами загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

До третій групи джерел загроз відносять явища, обставини, які майже неможливо спрогнозувати та відповідно запобігти (стихійні лиха). Це спонукає застосовуватися відповідні то цієї групи загроз завжди. Джерела загроз інформації, які виникають у наслідок стихійних лих, переважно є зовнішніми відносно об’єкту захисту.

Для підготовки обґрунтування політики безпеки або внутрішнього режиму щодо обігу інформації необхідно провести класифікацію вразливостей безпеки інформації. Небезпеки щодо інформаційної діяльності будь-якої установи, як можливі будь-які дії, спрямовані проти об’єкта захисту, можуть проявляються через вразливості, що призводять до зниження рівня безпеки інформації на конкретному об’єкті. Вразливості, як властиві об’єкту інформаційної діяльності, є властивими для нього та виникають через можливі недоліки у процесах функціонування, структурі установи, вимогах законодавчих (нормативних) документів, а в інформаційно-телекомунікаційних системах (автоматизованих системах) в наслідок архітектури, протоколів обміну та інтерфейсами, програмного забезпечення і апаратної платформи, умовами експлуатації та розташування. Відповідно, з метою реалізації своїх зловмисних завдань (порушення безпеки інформації) джерела загроз використовують вразливості. При цьому необхідно зауважити, що джерела загроз намагаються використати відповідні ті чи інші вразливості. Таким чином кожній загрозі можуть бути зіставлені різноманітні співставленні з ними вразливості.

об’єктивні вразливості

Вразливості безпеці інформації

суб’єктивні вразливості

випадкові вразливості

**Рис. 2.1. Види вразливостей безпеці інформації**

*Джерело*: складено автором на основі наукових публікацій [36].

Вразливості безпеці інформації поділяються на: об’єктивні, суб’єктивні, випадкові. Проведемо характеристику кожного з вказаних видів. Об’єктивні вразливості, як правило., обумовлені побудовою структури, організацією діяльності установи, а у випадках при дослідженні інформаційно-телекомунікаційних систем технічними характеристиками обладнання, що використовуються на об’єкті. Суб’єктивні вразливості виникають в наслідок дій співробітників та залежать від проведених працівниками маніпуляцій. Випадкові вразливості виникають залежно від середовища (її особливостей), в якому функціонує об’єкт захисту, та непередбачених обставин.

Загальноприйнятої єдиної класифікації загроз не існує, разом з цим існує багато її варіантів. Перелік тем подібних класифікацій, як приклад можливо привести наступні: по принципу впливу на систему, по характеру дії на систему, по меті реалізації, по причині виникнення помилки захисту, по типу дії атаки на об’єкт, по об’єкту впливу, по застосованих засобах атаки, по стану перебування об’єкту атаки. Також прийнято поділяти загрози на випадкові (або ненавмисні) і навмисні.

Детальніше проведемо їх аналіз. Перші можуть виникати в наслідок не навмисних дій персоналу: через помилки в забезпеченні, виходи з ладу технічних засобів, неправильні дії виконавців (користувачів), керівництва (адміністрації інформаційно-телекомунікаційних систем, мереж) і т.ін. Навмисні загрози, на відміну від випадкових, мають мету причинити шкоду і, в свою чергу, поділяться на активні і пасивні. Пасивні загрози спрямовані на несанкціоноване використання інформації (інформаційних ресурсів), не впливаючи на функціонування системи. Активні загрози спрямовані на порушення нормального функціонування системи документообігу (інформаційно-телекомунікаційної системи, локальної обчислювальної мережі та т.ін.) шляхом цілеспрямованого впливу на складові системи (в тому числі й апаратні, програмні і інформаційні ресурсів тощо).

Види загроз інформації

випадкові загрози

навмисні загрози

активні загрози

пасивні загрози

**Рис. 2.2. Види загроз інформації**

*Джерело:* складено автором на основі наукових публікацій [36].

Пропоную зупинитись на основних можливих варіантів порушення безпеки інформації, а саме:

* несанкціонований доступ — від доступу до відомостей, що відбувається в порушення режиму доступу (встановлених правил розмежування доступу в АС);
* витік інформації — наслідок дій порушника, при яких інформація стає доступною особам, право які не мають для цього;
* втрата інформації — дія, внаслідок якої інформація перестає існувати для осіб, які мають право власності на неї;
* підміна інформації —дії навмисного характеру при яких відбувається перекручення відомостей;
* блокування інформації — дії, що спричиняють перешкоджання доступу до інформації;

При цьому охарактерезуємо основні причини, які призводять до таких випадків, необхідно зазначити:

* виведення з ладу обладнання, кабельної мережі, перебої в електроживленні, збої серверів, робочих станцій тощо;
* некоректна робота програмного забезпечення (втрата або зміна даних при виникненні помилок у прогамному забезпечені, втрати інформації при заражені комп'ютерної системи вірусними програмами);
* навмисні дії сторонніх осіб (несанкціоноване знищення, копіювання, підробка чи блокування інформації, порушення роботи КС, спричинення витоку інформації);
* помилки персоналу, користувачів (не навмисне знищення, змінювання даних; некоректне використання апаратного забезпечення та комп’ютерних програм, яке має наслідком збоїв коректній роботі системи, виникнення небезпечних місць, недотримання інтересів законних користувачів тощо; неефективно влаштована система захисту; втрата інформаційних баз в наслідок їх некоректного зберігання тощо);
* дії персоналу навмисного характеру, зловмисників, ознайомлення сторонніх осіб із конфіденційною інформацією.

Значна частина можливих загроз інформаційної безпеки припадає на неналежний рівень так званої «культури інформаційної безпеки». Користувачі, умисно або через нестачу знання, є найбільшою загрозою для інформаційної безпеки. У роботі [54] М.Сіпонен зазначає, що без необхідних знань та співпраці користувачів з відділом безпеки або менеджменту адекватні засоби безпеки стають неефективними.

Акцентуючи увагу на людському фактор» необхідно розкрити визначення поняття «політики безпеки» (при використання інформаційно-телекомунікаційної системи для обробки інформації з обмеженим доступом) та режиму секретності (для обігу секретної інформації поза інформаційно-телекомунікаційної системи). Під політикою безпеки інформації розуміється набір правил, обмежень, рекомендацій тощо, які встановлюють правила обігу інформації і спрямовані на забезпечення захисту інформації від можливих загроз [10; 55]. Термін «політика безпеки» може бути застосований до організації, інформаційно-телекомунікаційної системи, операційної системи, послуги, що реалізується системою (або набору функцій) для захисту від визначених загроз, і т. ін. Для менших по розмірам об'єктів політика безпеки містить правила більш конкретніші й формальніші. Політика безпеки інформації в інформаційно-телекомунікаційній системі є частиною загальної політика безпеки організації, а також відбивають у собі й положення державної політики у сфері захисту інформації. При розробці політики безпеки включають та враховують загрози, каналу впливу, об'єкти атак.

[Режим](https://zakon.rada.gov.ua/laws/show/3855-12?find=1&text=%D1%80%D0%B5%D0%B6%D0%B8%D0%BC+%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%96" \l "w1_3) [секретності](https://zakon.rada.gov.ua/laws/show/3855-12?find=1&text=%D1%80%D0%B5%D0%B6%D0%B8%D0%BC+%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%96#w2_8) - встановлений згідно з вимогами Закону «Про державну таємницю»та інших прийнятих згідно до його вимог нормативно-правових актів єдині встановлені правила убезпечення охорони державної таємниці [48]. Власно, саме не дотримання регламентованих політикою безпеки та режим секретності в більшості й приводить до витоку інформації, рівно як й до втрати інформаційних ресурсів або збоїв (порушень) в роботі.

В залежності від фізичних властивостей носіїв інформації під час діяльності установи можливе утворення каналів витоку інформації. Розкриємо та скорочено дамо характеристику основним каналам фізичного витоку інформації:

1. Електромагнітний канал (утворюються в наслідок наявності магнітних полів, пов'язаних з протіканням електричного струму в технічних засобах інформаційно-телекомунікаційної системи. Електромагнітний канал, в свою чергу, поділяється на наступні види канал: радіозв’язку (високочастотне випромінювання), низькочастотний, мережевий (наводки у мережі електричного живлення), заземлення (наводки на елементи системи заземлення), лінійний канал (наводки на мережу зв'язків поміж ПЕОМ).

Причини утворення технічних каналів витоку інформації

недосконала елементна база

недосконалість схемних

рішень

експлуатаційна

зношеність

зловмисні

дії

конструктивних

зміна

характеристик

блокування засобів захисту

технологічних

зміна

характеристик

аварійний

вихід зі строю

створення аварійної

ситуації

**Рис. 2.3. Класифікація причин утворення технічних каналів витоку інформації**

*Джерело:* складено автором на основі наукових публікацій [36].

2. Акустичний (віброакустичний) канал (виникає шляхом поширення акустичних хвиль та пружних збурень в інших середовищах, в тому числі й які виникають при роботі засобів відображення інформації інформаційно-телекомунікаційної системи.

3. Візуальний (оптичний) канал (отримання інформації з використанням оптичних засобів: електромагнітне випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектра).

4. Матеріально-речовий канал (папір, фото, магнітні носії, відходи і т.д.)

Окремо необхідно зупинитись на технічних каналах витоку інформації з обмеженим доступом. Щоб впоратись із швидко наростаючим потоком інформації установи вимушені постійно нарощувати свій технічний арсенал обробки інформації. При його застосуванні в навколишньому середовищі створюються побічні електромагнітні, акустичні та інші випромінювання, які в тій чи іншій мірі пов’язанні з фізичними процесами, що відбуваються в таких пристроях при обробці інформації.

Джерела утворення технічних каналів витоку інформації

акустичні перетворювачі

акустичні перетворювачі

акустичні перетворювачі

* індуктивні
* ємкісні
* п’єзоелектричні
* оптичні
* низькочастотні
* високочастотні
* оптичні
* зворотній зв'язок
* по ланцюгах живлення
* по ланцюгах заземлення

**Рис. 2.4. Класифікація джерел створення технічних каналів витоку інформації**

*Джерело:* складено автором на основі наукових публікацій [36].

Такі випромінювання можуть поширюватись на значні відстані (до сотень метрів), що й може використовуватися зловмисники для перехоплення повідомлень з обмеженим доступом. Тобто наявність каналів витоку інформації впливає на вибір способу скоєння злочину. Перерахуємо їх:

* традиційні канали витоку аудіо- та відео- інформації;
* контактне або безконтактне підключення до електропристроїв;
* вбудовані мікрофони, відео- та радіо- закладки в стінах, меблях та предметах;
* знімання акустичної інформації за допомогою лазерних пристроїв з відображаючих поверхонь;
* оптичний дистанційний збір відеоінформації;
* застосування вузьконаправлених мікрофонів і диктофонів;
* витік інформації по ланцюгах заземлення, мереж гучномовного зв'язку, охоронної та пожежної сигналізації, лініям комунікацій та електромереж;
* високочастотні канали (побутової та іншої техніки);
* витік за рахунок поганої звукоізоляції стін і перекриття;
* дослідження зловмисником виробничих і технологічних відходів;
* витік інформації через телефонні та факсимільні апарати.

Середовище

розповсюдження інформаційних сигналів

Засоби технічної розвідки

Джерело інформаційних сигналів

Джерело перешкод

**Рис. 2.5. Модель технічного каналу витоку інформації**

*Джерело:* складено автором на основі наукових публікацій [36].

При деталізації складу каналу витоку інформації можливо відокремити окремі складові: технічні засоби обробки секретної інформації, середовище розповсюдження паразитних електромагнітних або інших випромінювань, засіб перехоплення і первинної обробки побічних (паразитних) випромінювань (рисунок 2.5).

Поширення сигналів, які можуть нести інформаційну складову, відбувається у середовище, яке можливо представити вільним простором з параметрами, що враховують природні ослаблення електромагнітних полів екранами, стінами будівель і приміщень, речами тощо, що знаходяться на шляху між технічним засобом і системи перехоплення, а також у вигляді дротів, ліній кабелів зв'язку і металевих конструкцій систем життєзабезпечення (водо-, газо-, електропостачання і центрального опалення), що виходять за межі контрольованих зон. Крім того, середовищем розповсюдження можливо виступати й ґрунт в районі закладення контурів заземлення.

Система перехоплення складається, як правило, з приймального пристрою, узгодженого фільтру і аналізатору, які забезпечують, відповідно, виявлення і найкращі умови для відокремлення інформаційної складовой випромінювання, обробку даного виду сигналу з метою забезпечення її “розбірливості”.

Поля, які утворюються струмами електричних зарядів в радіоелектронних приладах, є першопричиною побічних зв'язків і наведень. Вплив побічних полів через провідники й резистори одних вузлів і блоків на сигнали інших блоків і вузлів викликає паразитні зв'язки й наведення як усередині радіоелектронних приладів, так і між різними приладами, які розташовані поруч. Таким чином створюються загрози для інформації, яка міститься в інформаційних параметрах сигналів, що циркулюють в радіоелектронному приладі. Відповідно будь-який радіоелектронний прилад слід розглядати як можливе джерело загрози безпеки інформації. У природі відомі три види паразитного зв'язку, а саме: ємнісний (виникає під впливом електричного поля), індуктивний (виникає під впливом магнітного поля), гальванічний (як наслідок загального активного опору). Крім електромагнітних полів при вирішенні питань захисту інформації необхідно розглядати й акустичні поля у діапазоні, які сприймаються на слух.

Мова є одним з найдавніших способів обміну інформацією між людьми. Технічний прогрес дозволяє сьогодні використовувати широку низьку засобів передачі і зберігання інформації. Проте і в наш час зацікавленість викликає контроль інформації у мовному вигляді, живої розмови.

Це викликано цілим рядом специфічних особливостей, які притаманні саме мовній інформації і пов'язані з деякими рисами людської психіки:

а) конфіденційність;

б) оперативність;

в) віртуальність.

Перехоплена мовна інформація – це як документом, особисто підписаний людиною, який озвучив повідомлення, оскільки сучасні методи аналізу мови дозволяють ідентифікувати його особу. Зазначені особливості мовної інформації пояснюють її важливість, а відповідно й високу зацікавленість в її перехоплені.

Пропоную розглянути технічних каналів витоку інформації. Для перехоплення акустичних сигналів, які поширюються повітрям використовуються мікрофони (високочутливі і спеціально спрямовані) по повітряному каналу витоку інформації. Мікрофони під’єднуються до портативних звукозаписних або спеціальних мініатюрних передаючих пристроїв. Пристрій у автономному вигляді, якій об'єднує в собі мікрофон і передавач, прийнято називати закладним пристроєм перехоплення мовної інформації. При цьому інформація, яка перехоплена закладним пристроєм може передаватись по різних каналам: радіоканалу, мережі електроживлення, інфрачервоному каналу, з'єднувальним лініях будь-яких технічних засобів, інженерних комунікацій в ультразвуковому діапазоні частот, телефонній лінії.

Відповідно прийом інформації від закладного пристрою відбувається на спеціальні приймальні пристрої у відповідному діапазоні довжин хвиль.

Проаналізуємо вібраційні технічні канали витоку інформації. Будівельні огороджувальні конструкції та інженерні комунікації (як то: труби систем опалення, водопостачання) є середовищем, по якому поширюються мовні сигнали. В даному випадку для зняття інформації використовуються вібродатчики. В свою чергу перехоплена інформація може передаватись по різних каналам: в основному радіоканал (пристрій перехоплення називається радіостетаскопами), або по оптичному каналу в ІЧ діапазоні, а також з ультразвукового каналу (з інженерних комунікацій).

Використовується також й електроакустичні технічні канали витоку інформації, які виникають за рахунок перетворення акустичних сигналів в електричні. Деякі елементи радіотехнічних пристроїв, такі як трансформатори, котушки індуктивності, електромагніти дзвінків телефонних апаратів, мають властивості змінювати свої фізичні параметри (ємність, індуктивність, опір) під дією тиску акустичної хвилі. Крім зазначених елементів, прилади можуть містити в своїх схемах акустоелектричні перетворювачі: деякі типи датчиків пожежної, охоронної сигналізації, гучномовці ретрансляційної мережі. Такий ефект акустоелектричного перетворення називають мікрофонним. Перехоплення зазначених коливань в даному каналі витоку здійснюється шляхом з'єднання до ліній підключення вказаних пристроїв спеціальних високочутливих низькочастотних підсилювачів.

Розглянемо черговий оптико–електронний технічні канали витоку інформації. При опроміненні лазерним променем поверхонь конструктивних елементів, які огороджують приміщення, відбувається модуляція під дією акустичного мовного сигналу. Відбите лазерне випромінювання модулюється (по амплітуді, фазі) і приймається приймачем, при демодуляції відокремлюється мовна інформація. Для перехоплення інформації використовуються лазерні мікрофони, які працюють в ІЧ діапазоні.

Разом з цим параметричний канал витоку інформації може бути утворений й шляхом "високочастотного опромінення" приміщення, де завчасно змонтовані напівактивні закладні пристої, які мають елементи, деякі характеристики яких змінюються під впливом акустичного (мовного) сигналу.

При цьому зняття інформації у мовному вигляді по прямому акустичному та віброакустичному каналах залишається одним з найбільш результативним способів такого перехоплення.

Виходячи з зазначеного вище для оптимізації вирішення поставленого завдання можемо підсумувати що канали витоку інформації поділяються на ті що відносяться до технічних (при явищах, заходах виробничого процесу, які по’вязані з використанням технічних засобів обробки інформації) та не технічних (т.е. дії персоналу, заходи виробничих процесів, які здійснюються без використання технічних засобів обробки інформації).

**2.2. Моніторинг каналів витоку інформації**

Важливість питання безпеки інформації підтверджує поширена практика наявності у структурі установи підрозділів, які розробляють та впровадження політики безпеки. Повсякденний контроль щодо забезпечення безпеки інформації з обмеженим доступом здійснюється окремими підрозділами (окремими посадовими особами), за якими закріплені відповідні функції з режиму секретності та технічного захисту інформації, а також утвореними у підрозділах службами захисту інформації в інформаційно-телекомунікаційній системі. На виконання вимог ст. 21 Закону України «Про державну таємницю» №3855-12 від 21.01.1994 (Закон № 3855-12) «в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, …… створюються на правах окремих структурних підрозділів режимно-секретні органи...» [47].

Таким чином на законодавчому рівне визначений статус цих підрозділів на правах структурного (основного) підрозділу установи, з підпорядкуванням «… безпосередньо керівнику ...» [47].

По питаннях реалізації безпекової політики в державі, рівно як й в відомстві (галузі) режиму секретності режимно-секретний орган керується вказівками вищестоящого подібного органу.

Законом № 3855-12 встановлена мета цього утворення, як «…розроблення та впровадження заходів щодо здійснення режиму секретності, контролю за їх втіленям…» в установі [47].

Службою безпеки України, як «Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці.. погоджується створення, реорганізація чи ліквідація режимно-секретного органу.

У своїй роботі режимно-секретні органи взаємодіють з органами Служби безпеки України. » [47].

Закон № 3855-12 визначає й основні завдання цих підрозділів. Серед широкого переліку цих завдань для розкриття питань теми кваліфікаційної роботи необхідно виділити окремі з ним:

«… запобігання розголошенню секретної інформації, виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів,…

…здійснення контролю за станом режиму секретності, …

…..здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності у підрозділах державного органу…» [47].

Передача функцій режимно-секретного органу будь-яким іншим підрозділам не допускається [47]. Крим Закону № 3855-12 існує ціла низка інших Законів України та підзаконних актів щодо напрямків діяльності режимно-секретного органу.

Таким чином, законодавством визначаються правові аспекти впровадження загальнодержавної політики у сфері безпеки інформації в тому числі й шляхом покладання відповідальності та зобов’язань на спеціально утворені підрозділи – режимно-секретні органи, або окремих посадових осіб. Низькою нормативних документів, щодо регламентації діяльності режимно-секретного органу передбачена їх планова діяльність, періодичність здійснення  планових  заходів в тому числі щодо контролю стану та положення з питань безпеки інформації в установі. Серед інших питань контролю є виявлення можливих каналів витоку інформації, вироблення своєчасних заходів щодо їх блокування, оцінка рівня вжитих заходів захисту, їх достатності, ефективності контроль за дотриманням вимог щодозахисту інформації.

Для запобігання утворення можливих каналів витоку інформації в установі повстає питання проведення ретельного дослідження наявних інформаційних процесів, тобто по суті всієї «виробничої» діяльності. Адже, прийняття будь-яких рішень, актів тощо - це результат роботи з наявною інформацією, - процес, якій скерований на збір, обробку та надання інформації керівництву, посадовим особам (суб’єктам, які приймають рішення), та в свою чергу створення нової інформації на базі існуючої у вигляді відповідного документу (наказу, розпорядження, акти, протоколу, листа тощо).

Елементом важливим для забезпечення організації діяльності установи є інформаційні комунікації між всіма структурними підрозділами та їх працівниками. Тому в сфері дослідження комунікативного забезпечення перебувають й процеси координації діяльності. Інформаційний ресурси – це банки даних, масиви документів, книг тощо, що є в інформаційних системах внаслідок збору та обробки інформації. Через інформаційні процеси відбувається використання наявної інформації. А тому одним з основних зусиль під час досліджень інформаційної безпеки необхідно зосередити на вивчення структури інформаційно-комунікаційної системи установи. Ця система має в своєму складі цілу низьку окремих частин: технічні засоби, засоби зв’язку (комунікації), мережі інформаційних служб (інформаційні відділи тощо), місця збереження носіїв інформації (архіви, бібліотеки, фонди тощо).

Сучасною наукою всі об’єкти, предмети, явища розглядаються як складові певної системи, тому для вивчення інформаційних процесів необхідно, на мою думку, застосовувати системний підхід. Інформація є об’єктом, обіг якого підлягає вивченню з метою визначення найбільш критичних місць у «виробничому процесі» з точки зору можливих порушень стандартів (правил) політики безпеки. Щодо інформаційних процесів, то без системного бачення і аналізу не можливо уявити можливість з’ясувати причини, наслідки і перспективи будь-яких подій і процесів. Цей процес дослідження повинен відбуватись з урахуванням всіх взаємозв’язків елементів системи, системного аналізу всіх можливих наслідків прогнозного розвитку ситуацій чи проблем.

Системний аналізу має особливість, що полягає в тому, що він дає можливість розкласти складну проблему на окремі компоненти аж до постановки конкретних завдань, щодо яких є методи їх вирішення, а, одночасно, зберігає всю цілісність проблеми. Аналіз системного характеру використовується для вирішення складних проблем, які пов'язані з діяльністю людей [4].

Наслідки реалізації загрози можуть впливати на інформацію як безпосередньо, так і опосередковано. При аналізі системи захисту інформації необхідно враховувати багато факторів, серед яких питома вага належить умовам використання технічних засобів. Загрози інформації залежать від характеристик внутрішньої системи діяльності установи, фізичного середовища, персоналу і оброблюваної інформації. Безпосередньо дослідження питань безпеки інформації в установі необхідно розпочинати, на мою думку, з вивчення завдань та функцій, які закріплені за установою Законами України, постановами та іншими нормативними документами. Виходячи з функцій визначають об’єкт захисту, а саме наявність інформації, що підлягає захисту, т.е. убезпечення від загроз. Для прийняття обґрунтованих рішень, проведення об’єктивної оцінки, необхідно з’ясувати види, форми, категорії інформації, способи та умови її обробки, та як наслідок якими нормативно-правовими актами встановлюється відповідні режими доступу та вимоги щодо умов її обігу.

В наслідок дослідження інформації підрозділами захисту інформації (режимно-секретні органі) складаються відповідні документи на доповідь керівництву щодо:

* опису інформаційної діяльності установи з зазначенням всіх процесів інформаційно-комунікаційного характеру, питань які можуть мати значення при вирішенні проблем безпеки інформації;
* переліки інформації з обмеженим доступом, яка підлягає захисту в установі, з зазначенням видів і місць її обігу, категорії (гриф секретності, ступень обмеження доступу).

Аналіз інформаційних потоків, інвентаризації інформаційних ресурсів та ранжирування інформації, яка оброблюється, передається або зберігається, за мірою її цінності керівництво установи одержує цілісну картину одного з найбільш складних об’єктів – інформаційної системи, що позитивно впливає на якість керування всіма процесами взагалі і, як наслідок, покращує його ефективність. Приміщення, місця циркуляції (обговорюється, пересилається, приймається, перетворюється, накопичується, відображається, і зберігається тощо) інформація з обмеженим доступом (об’єкти інформаційної діяльності) досліджуються внутрішньою комісією з метою визначення та присвоєння категорії в залежності від категорії відповідної інформації з обмеженим доступом.

Після проведення категорування складається перелік категорованих об’єктів інформаційної діяльності установи та внутрішньою комісією проводиться обстеження щодо наявних умов обігу інформації з обмеженим доступом (розташування, умови зберігання, розмежування доступу, наявні засоби, комунікації тощо) з наданням пропозицій щодо подальшої роботи з інформацією з обмеженим доступом або здійснення додаткових заходів щодо забезпечення безпеки інформації. За результатами роботи комісії керівнику установи подаються на розгляд відповідні акти.

Дослідження інформаційної діяльності установи

Опис інформаційної діяльності установи

Складання переліків інформації з обмеженим доступом, яка підлягає захисту

Визначення об’єктів інформаційної діяльності зі складанням переліку

**Рис. 2. 5. Документальне оформлення результатів проведення дослідження інформаційної діяльності**

*Джерело:* складено автором на основі нормативних документів у галузі технічного захисту інформації [22, 23, 24].

Всі зазначені питання вивчаються різноманітними методами, в комплексі, які доступні на момент роботи, як то:

* вивчення нормативних документи, що регламентують діяльність;
* анкети;
* спостереження за процесом повсякденної діяльності;
* безпосереднє спілкування з персоналом, опитування;
* дослідження наявних інформаційних баз, документів тощо.

Здійснюючи в комплексі аналіз «виробничої» діяльності установи, щодо виконання всіх завдань й функцій, які закріплені державою, необхідно відслідковувати причинно-наслідкові зв’язки тих чи інших дій і процесів, як між структурними підрозділами, у самих підрозділах, так й безпосередньо виконавцями (користувачами інформаційно-телекомунікаційної системи). Відповідно до законів та нормативно-правових актів з захисту інформації керівник установи, в якій обробляється інформація, до якої встановлені обмеження доступу та яка підлягає захисту згідно закону, забезпечує захист інформації в порядку та на умовах, визначених у Законах України та інших підзаконних актах. За наслідками проведеної роботи за пропозиціями підрозділу захисту інформації керівником установи приймається рішення щодо проектування та створення загальної системи захисту інформації та відповідні комплексні системи на кожному об’єкті інформаційної діяльності окремо. Ці вказані процедури повинні відбуватись на початковому етапі створення установи. В подальшому після приведення всіх питань інформаційної безпеки у відповідність до вимог нормативних документів в цій сфері відбувається постійний систематичний періодичний плановий контроль за дотримання встановлених у політиці безпеки вимог.

Загрози можуть мати як об'єктивну складову (зміна умов фізичного середовища, відмова елементів взаємодії системи) так і суб'єктивну - «людський фактор», який не завжди пов’язаний з нестачею або недосконалістю заходів захисту, але він завжди пов’язаний з недотриманням вимог політики безпеки. Звичайні помилки та непорозуміння визначається як інцидент безпеки, але як на них реагувати теж грає важливу роль.

**2.3. Практичні аспекти застосування методів виявлення загроз інформації**

Виходячи з загального уявлення щодо можливих загроз інформаційної безпеці установи (структура організації, інформаційні потоки між структурними підрозділами та зі зовнішніми організаціями, наявні об’єкти інформаційної діяльності та системи захисту інформації) підрозділами захисту інформації здійснюються заходи контролю періодично: планові, а також й поза планово (раптово). Контролю підлягають всі напрямки діяльності пов’язанні з інформаційним забезпеченням установи. Планування та організація контролю за станом захисту інформації поділяється на напрямки відповідно на охорону державної таємниці та технічний захист інформації. Ці питання розглядаються разом й в комплексі, але кожний напрямок має свою специфіку. В першу чергу це пов’язано з наявністю необхідності технічного контролю зі застосуванням контрольно-вимірювального обладнання під час дослідження рівня технічного захисту інформації. Контрольні заходи є перевірка відповідності фактичних дій (як правило, документальне підтвердження у визначених формах обліку здійснення цих дій) до вимог положень нормативних документів.

Розглянемо окремо основні практичні питання процесу контроля, який матиме сукупність таких етапів, підетапів. Всі роботи можна поділити на етапи: підготовчий, основний та заключний. Досліджуючи підготовчий етап зауважимо що включає в себе:

- вивченню та уточнення інформації щодо функціонування установи в цілому (положення про установу, її завдання та функції, інформація якого характеру використовується для вирішення цих завдань, види та обсяги цієї інформації, структуру, кількісний та якісний склад персоналу, наявність та кількість об’єктів інформаційної діяльності, їх види);

 - планування з визначенням основних питань, які підлягають дослідженню з визначенням часових показників;

При проведенні заходів основного етапу здійснюється перевірка відповідності нормативним документам фактичного виконання вимог на практиці.

З питань охорони державної таємниці необхідно досліджувати слідуючи аспекти:

* порядок обігу матеріальних носіїв секретної інформації;
* регламентація документально внутрішнього режиму доступу до матеріальних носіїв секретної інформації, відповідність його нормативним документам у галузі;
* присвоєння ступенів обмеження доступу матеріальним носіям секретної інформації;
* ведення секретного діловодства та архівне зберігання;
* контроль за секретними роботами;
* використання інформаційно-телекомунікаційної системи для підготовка матеріальних носіїв секретної інформації.

 Під час дослідження питань технічного захисту інформації пропоную зупинитись на таких ділянках:

* категоріювання об’єктів інформаційної діяльності (приміщень, які виділені для проведення закритих нарад, інформаційно-телекомунікаційної системи та інші технічні засоби, які призначені для обробки інформації з обмеженим доступом);
* здійснення заходів щодо захисту інформації організаціями, які отримали спеціальну ліцензію на діяльність у галузі технічного захисту інформації;
* виявлення контрольно-вимірювальними технічними засобами (комплексами) можливі технічні канали витоку інформації та визначення необхідних заходів щодо їх блокування;
* створення комплексної системи захисту інформації на підставі проектної документації, яка погоджується з відповідними органами;
* атестація об’єктів інформаційної діяльності по виконанню вимог захисту інформації (нормативні документи технічного захисту інформації, приписів по експлуатації технічних засобів тощо) під час здійснення робіт з інформацією з відповідною ступеню таємності;
* використання технічних засобів з сертифікатами відповідності, як основних та і допоміжних;
* встановлення контрольованої зони установі (об’єктів інформаційної діяльності);
* організація контролю і обмеження доступу на об’єкті інформаційної діяльності (у приміщення), їх фізична охорона;
* наявність інструкторських матеріалів (приписів) щодо дотримання політики безпеки інформації та доведення їх до персоналу, який залучається до робіт на об’єкті інформаційної діяльності,

На заключному етапі відпрацьовується проект звітного документу (акт перевірки, доповідь-довідка тощо). Звітні документи за підсумками здійснюваного контролю містять розділи, наявність яких передбачено внутрішніми розпорядчими документами відповідного відомства. Важливим й обов’язковим розділом звітного документу є висновки щодо відповідності рівня захисту інформації (здійснених заходів) вимогам норм розпорядчих документів, виявлені недоліки та пропозиції для їх усунення.

Велике значення для успіху є виконання необхідної умови щодо залучення кваліфікованих фахівців до організації захисту інформації. Це диктується тим, що тільки вони спроможні визначити всі загрози і знайти відповідні ефективні засоби протидії. Разом з цим до питань захисту інформації повинні залучатись весь персонал, користувачі, оскільки вказану задачу нема можливості вирішити лише технічними і програмними інструментами, людський фактор потужне впливає у дотримання режиму конфіденційності.

Тільки при використані інформації персонал може найкраще оцінити важливість її щодо встановлення заходів адекватного рівня з її захисту. Відповідно цей персонал приймає активну участь у розробці та вдосконалені політики захисту, в наслідок того що остання є складовою частиною внутрішнього режиму установи, організації.

**Висновки до розділу 2**

Підсумовуючі зазначене можливо дійти висновку, що у сучасним умовам діяльності установ державної системи управління притаманне велике різноманіття інформаційних ресурсів. Ця інформація перебуває у різних формах та видах, постійно перебуває у русі. Органи державної влади при цьому підтримують зв’язки з іншими установами, організаціями, громадянами, що обумовлює обмін як окремими документами так великими масивами інформаційних ресурсів. Проведення в останній період часу прискореної цифрової трансформації суспільства ї публічного управління викликало необхідність вирішення питань надання доступу до інформаційних ресурсів (реєстрів) між різними державними органами.

Це все разом з різноманіття видів виробничих процесів, їх форм, різних типів технічних засобів обробки, передачі інформації створює велику кількість можливостей для зловмисників, як і їх варіантів втрати, розголошення інформації, яка використовується в установі.

Разом з тим необхідно пам’ятати, що постійний розвиток науки та технологій призводить до удосконалення технічних засобів та способів несанкціонованого здобуття (зняття) інформації, що приводить до відповідних змін у переліку можливих каналів витоку інформації.

**Розділ 3**

**Шляхи запобігання загрозі безпеки інформації органів ДФС України**

**3.1. Напрямки вдосконалення інформаційної діяльності та методів її захисту**

Державна фіскальна служба при здійснені встановлених завдань керується [Конституцією](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80) та Законами України, Указами Президента України та Постановами Верховної Ради України, прийнятими відповідно до Конституції та Законів України, актами Кабінету Міністрів України, іншими актами законодавства, Положенням про Державну фіскальну службу України (затверджено Постановою Кабінету Міністрів України від 21 травня 2014 р. № 236) [37].

Головне управління Державної фіскальної служби у Тернопільській області утворено на виконання Положення про Державну фіскальну службу України (Постанова Кабінету Міністрів України від 21 травня 2014 р. № 236).

У своїй діяльності керується у відповідності до Положення про Головне управління ДФС у Тернопільській області (наказ ГУ ДФС у Тернопільській області від 01 лютого 2019 р. № 80) Конституцією та Законами України, Указами Президента України, Постановами Верховної Ради України, прийнятими відповідно до Конституції та Законів України, наказами Мінфіну, що належать до компетенції ДФС, наказами ДФС, дорученнями Голови ДФС, його першого заступника та заступників, іншими законодавчими актами.

Підрозділи податкової міліції у складі ДФС на виконання пункту 4 Постановою Кабінету Міністрів України від 25.09.2019 № 846 «Про внесення змін до деяких актів Кабінету Міністрів України» виконує функції щодо боротьби з правопорушеннями у сфері застосування податкового законодавства, здійснює оперативно-розшукову, кримінальну процесуальну та охоронну функції, що віднесені до його підслідності згідно положень Кримінального процесуального кодексу України.

На всіх етапах реалізації завдань та функцій ДФС, як й у будь-якому іншому державному органі, відбувається постійний збір, обробка інформації, моніторинг, систематизація та її аналіз, збереження та використання для прийняття управлінських рішень. Без необхідної інформації у відповідному вигляді (на різних матеріальних носіях, паперовому, електронному, акустичному вигляді тощо) неможливо виконання жодного функції або завдання, які покладаються на установу. Таким чином, інформація визнана найважливішим ресурсом управління [17].

Відповідно до визначених завдань Головне управління ДФС в області утворюється з відповідних структурних підрозділів (рисунок 3.1.). Переважна частина працівників проходить службу на атестованих посадах, які пов’язані безпосередньо з виконанням діяльності щодо запобіганням кримінальних правопорушень у сфері оподаткування. До цих підрозділів відносяться слідче управління фінансових розслідувань та управління боротьби з фінансовими злочинами.

За слідчим управлінням фінансових розслідувань закріплені наступні завдання: виявлення обставин, що можуть свідчити про кримінальне правопорушення та реагування згідно до чинного законодавства; розшук осіб, які знаходяться під слідством та судом з кримінальних правопорушень у галузі оподаткування, митній та бюджетній сферах; проведення діяльності оперативно-розшукового характеру, заходів щодо досудового розслідування та відшкодування державі завданих збитків. згідно норм закону.

Управління боротьби з фінансовими злочинами відповідає разом з іншими напрямками діяльності за: виявлення правопорушень кримінальних та інших у сферах оподаткування, митної та бюджетної політики, а також встановлення місця перебування платників податків, опитування засновників підприємств, посадових осіб; розшук осіб, які перебувають під слідством та судом за кримінальні правопорушення у сфері оподаткування, митній та бюджетній галузях.

Начальник Головного управління ДФС області

Перший відділ розслідування кримінальних проваджень

Заступник начальника ГУ – начальник Управління боротьби з фінансовими злочинами

Сектор забезпечення діяльності Служби

Сектор роботи з персоналом

Сектор фінансово-бухгалтерського забезпечення

Сектор правового забезпечення

Сектор матеріально-технічного забезпечення

Сектор внутрішньої безпеки

Спеціаліст запобігання та виявлення корупції

Сектор аналітичної роботи, прогнозування та оцінки ризиків

Відділ координаційного забезпечення податкової міліції

Заступник начальника ГУ - начальник Слідчого управління фінансових розслідувань

Другий відділ розслідування кримінальних проваджень

Сектор захисту інформації

Відділ організації викриття економічних злочинів та боротьби з відмиванням доходів, одержаних злочинним шляхом

Сектор організації оперативно-розшукової діяльності

Відділ протидії злочинам у сфері обігу товарів акцизної групи

Сектор викриття кримінальних правопорушень у зовнішньоекономічній сфері

Оперативно-технічний відділ

Міжрегіональний відділ оперативного документування

**Рис. 3.1. Структура Головного управління ДФС області**

*Джерело:* складено автором на основі Положення про ДФС [52]

До складу ГУ ДФС області входять також підрозділи, які забезпечують функціонування установи в цілому (якби мовити, «допоміжні»), але непов’язані безпосередньо з правоохоронною діяльністю.

Закріплення розподілу основних функцій за структурними підрозділами Головного управління ДФС в області відбувається у відповідності до положення про установу (табл. 3.1).

*Таблиця 3.1.*

**Розподіл основних функцій за структурними підрозділами**

**Головного управління ДФС в області**

|  |  |
| --- | --- |
| Назва структурного підрозділу  | Окремі основні функції |
| Керівництво   | Загальне керівництвоВтілення інституційних змін здійснення діяльності ДФС та проектів у ДФС, її територіальних органахУчасть у стратегічному плануванні розвитку ДФС |
| Сектор забезпечення діяльності Служби  | Організація роботи, функціональне, структурне забезпечення, координація діяльності ГУ Поточне планування діяльності ГУОрганізація (участь в організації) засідань Колегії ГУЗагальне діловодство, електронний обмін службовими документамиЗдійснення перевірок з окремих питань за дорученням керівника ГУ Забезпечення доступу до публічної інформації |
| Сектор охорони державної таємниці | Забезпечення охорони державної таємниціЗабезпечення технічного захисту інформації та контролю за його станомОрганізація захисту інформації та контроль рівня його стану |
| Слідче управління фінансових розслідувань | самостійне виявлення з різних будь-яких джерел обставин, що можуть засвідчувати про здійснення кримінального правопорушення та вжиття відповідних заходів, передбачених чинним законодавством;Розшук осіб, які перебувають під слідством та судом за кримінальні правопорушення у галузі оподаткування, митній сфері та бюджетній Здійснення у межах закону повноважень оперативно-розшукової діяльності, досудового розслідування та заходів щодо відшкодування завданих державі збитків |
| Управління боротьби з фінансовими злочинами  | Виявлення кримінальних та інших правопорушень у сфері оподаткування, митній та бюджетній сферах.Розшук осіб, які переховуються від слідства та суду за кримінальні правопорушення у сфері оподаткування, митній та бюджетній сферахПроведення в межах наданих законом повноважень оперативно-розшукової діяльності, досудового розслідування. |
| Сектор роботи з персоналом | Здійснення добору кадрів в ГУ, формуванні державного замовлення на допідготовку фахівців у потрібних сферахКонтроль за виконанням Правил поведінки посадовими особами ГУ  |
| Сектор фінансово-бухгалтерського забезпечення | Ведення бухгалтерського обліку та складання звітності ДФСВедення обліку трудових ресурсів та заробітної плати |
| Сектор правового забезпечення | забезпечення своєчасного проведення заходів та процедур, пов’язаних з припиненням (ліквідацією, реорганізацією) платників податків у межах компетенції; Забезпечення законності діяльності ГУ,Представництво інтересів у судах |
| Сектор матеріально-технічного забезпечення | Адміністративно-господарська діяльність, участь в організації державних закупівель, транспортне, матеріально-технічне забезпеченняПідтримання пожежної, техногенної безпеки, мобілізаційної готовності, мобілізації, цивільного захисту і охорони праціФормування та ведення баз даних ГУ Адміністрування та супроводження роботи телекомунікаційних систем, мережевих сервісів, серверного приміщення |
| Спеціаліст запобігання та виявлення корупції | Втілення роботи щодо запобігання корупції згідно до вимог антикорупційного законодавства |

*Джерело:* складено автором на основі Положення про ДФС [52]

У питаннях боротьби з правопорушеннями у своєї сфері ДФС дотримується положень КПКУ. Розділ ІІІ КПКУ розкриває положення досудового розслідування, в тому числі зміст негласних слідчих (розшукових) дій.

Стаття 246 глави 21. КПК зазначає: «негласні слідчі (розшукові) дії - різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених цим Кодексом:

* відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати в інший спосіб
* виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів».

На всіх етапах проведення процесуальних дій працівники податкової міліції здійснюють документоване супроводження. За результатами цієї діяльності утворюється документи різного характеру, зміст та форми яких суворо регламентовані відповідними нормативними вимогами. Так само визначено й порядок обігу їх як в установі (між підрозділами, посадовими особами) та й поза межами установи (адресовані до інших установ, організацій та громадян).

Схематично обіг документів (на паперовому носії і в електронному вигляді) можливо представити схематично (рисунок 3.2).

Прийом документів

Відправлення вихідних документів

Попередній розгляд

Реєстрація

Маршрутизація

Нагадування про доручення

Розгляд керівником

Обговорення погодження

Прийом документів

Підготовлені документи

Внутрішні документи

Скерування документа виконавцю

Контроль виконання доручення

Виконання документів (доручення)

Долучення документів до справ, місць зберігання

Знищення

Подальше виконання

Направлення до архіву

**Рис. 3.2. Порядок документообігу в установі**

*Джерело:* складено автором на основі службових інструкцій установи.

Для підготовки будь-яких матеріалів (документів) в сучасних умовах застосовуються технічні засоби обробки та передачі інформації: автоматизованої системи, інформаційно-телекомунікаційної системи, копіювальна техніка та т.ін. Паралельно відбувається обговорення, доповіді окремих службових питань керівництву. Під час всіх зазначених дій циркулює інформація в різних формах та виглядах: акустичному, електронному та паперовому. Впровадження в останні рокі електронного документообігу привело до значного збільшення загроз інформаційній безпеці у вигляді виникнення додаткових можливостей для копіювання, крадіжки або блокування, знищення ресурсів інформації з обмеженим доступом. Способи здійснення цих злочинних дій в загальному нарисі були розгляну в попередній частині роботи. Спираючись на перелік загроз для інформаційної діяльності в установі розробляються та запроваджуються необхідні заходи

Розглянемо більш докладно основні методи захисту інформаційних ресурсів установи. Варіанти організації захисту інформації (склад системи захисту інформації), безпосередньо залежать від цілої низки факторів. До них можливо віднести: категорії інформації, яка обробляється в установі, та вимог керівних документів щодо захисту цієї категорії інформації, в якому вигляді та яких обсягах інформація циркулює в установі, технічних показників можливих для використання засобів захисту інформації, можливостей фінансових витрат на захист інформації.

Основні принципи запобігання витоку інформації пропоную звести до слідуючих:

* суворий облік (матеріальних носіїв секретної інформації, виробничих процесів, дій виконавців, користувачів);
* створення умов зберігання, доступу, використання інформації (в будь-якому вигляді та формі);
* контроль на всіх етапах обігу інформації з обмеженим доступом (постійний, періодичний, раптовий, комплексний або з окремих питань).

Чисельні заходи щодо усунення реалізації інформаційних загроз об'єднують по групах:

1. Законодавчі (правові) - чинні закони, укази, нормативні акти, які регламентують вимоги щодо поводження з інформацією, матеріальними носіями інформації, а також й відповідальність за порушення цих вимог.

2. Морально-етичні - норми поведінки, які складаються при зростанні громадянського суспільства, укріпленні державних інститутів, поширені комп'ютерної техніки. Недотримання встановлених норм приводить до падіння авторитету установи, держави, людей.

3. Організаційні - заходи адмінітрстивного характеру, які встановлюють процеси функціонування установи, інформаційно-телекомунікаційної системи, діяльність працівників з метою максимального запобігання можливості реалізації загроз безпеки. До них відносяться:

* контроль за діяльністю персоналу;
* облік зберігання, використання, знищення документів і носіїв інформації;
* охорона контрольованої зони та пропускний режим;
* підбор і підготовка персоналу;
* дотримання вимог щодо надання доступу до інформації;
* впровадження технічних засобів захисту інформації та ПЗ.

4. Фізичні - застосування технічних засобів охорони і інженерних споруд, які призначені для створення фізичних перешкод на шляхах доступу в контрольовану зону.

5. Технічні - використання технічних пристроїв і програм, що входять в склад інформаційно-телекомунікаційної системи і виконують функції захисту (засоби аутентифікації, апаратура шифрування та т.ін.).

Самі механізми захисту інформації реалізуються на трьох рівнях з врахуванням існуючих загроз: фізичному, особистісному та організаційному.

Визначення переліку можливих загроз інформаційної безпеки установи робиться фахівцями на підставі ретельного аналізу відомостей про:

* наявні інформаційні ресурсів (їх категорії, вигляд, обсяг, вимоги щодо зберігання, поводження, надання доступу);
* структуру, завдання і функції установи;
* порядок проходження інформаційних потоків в установі (між підрозділами, посадовими особами) та на зовні (аналізуючи середовище функціонування);
* наявні технічні засоби обробки та передачі інформації та їх застосування в інформаційній діяльності;
* модель загроз, модель порушників
* розробляються та впроваджуються відповідні заходи.

Для більшої ефективності роботи необхідно застосовувати системний підхід, що означає: одночасне впровадження засобів захисту інформації під централізованим управлінням, створення такого середовища обробки інформації, що об’єднує різноманітні заходи для протидії загрозам (правові, організаційні, програмно-технічні). При цьому складові в системи повинні взаємодіяти та забезпечувати захист таким чином щоб протидіяти загрозам як внутрішніх так і зовнішніх.

До переліку робіт з захисту інформації пропоную включити наступні заходи:

1. створення та функціонування спеціалізованого підрозділу (призначення відповідальної посадової особи);
2. система обмеження фізичного доступу до контрольованої зони (інженерно-технічні обладнання, охорона, розміщення, організація доступу до відповідних приміщень, об’єктів інформаційної діяльності);
3. секретне діловодство та інші складові режиму секретності;
4. комплекс технічного захисту інформації (інформація в акустичному вигляді);
5. комплексна система захисту інформації (інформаційно-телекомунікаційні системи);
6. криптографічний комплекс засобів захисту (реалізується, як за допомогою програмних засобів, так і апаратних засобів);
7. регламентація дій персоналу на всіх ділянках діяльності.

Як зазначалось вище, організація забезпечення безпеки інформації повинна носити не просто комплексний характер, але ще й ґрунтуватися на всебічному аналізі можливих негативних наслідків та планування необхідних заходів щодо їх усунення. Досвід вирішення завдань інформаційної безпеки державних органах в сучасних умовах показує, що при всіх можливих відмінностях існують обов'язкові напрямки та умови захист інформації. Ця діяльність здійснюються за наступними аспектами. Розглянемо докладніше необхідність наявності спеціалізованого підрозділу в установі для вирішення питань безпеки інформації. З метою організації та здійснення заходів щодо забезпечення інформаційної безпеки в установі створений Підрозділ захисту інформації.

До посадових обов'язків персоналу цього підрозділу входить завдання щодо впровадження, в першу чергу, таких організаційних заходів:

* визначення пріоритетних напрямків захисту інформації з урахуванням можливих загроз та специфіки діяльності установи;
* розробка комплексного плану захисту інформації;
* втілення і контроль за виконанням регламентів розмежування доступу до інформаційних ресурсів (баз даних) в залежності від функціональних обов’язків конкретного працівника, та оформлення відповідних процедурних документів щодо допуску за погодженням з відповідними контролюючими органами (підрозділами);
* розробка та супроводження (контроль) докладних інструкцій та правил, які регламентують порядок роботи працівників та поводження з секретною (конфіденційною) інформацією та матеріальними носіями тощо;
* забезпечення необхідного рівня технічного захисту інформації на всіх об’єктах інформаційної діяльності установи.

Це неповний перелік напрямків діяльності в узагальненому вигляді. Зусилля фахівців, які задіяні в установі по вирішенню питань захисту інформації, мають за мету створення високоефективної системи управління всіма компонентами, інструментами та засобами цілої системи захисту інформації на всіх стадіях обігу документів задля запобігання утворення будь-яких можливих каналів витоку інформації.

Сучасні тенденції потребують застосування відмінних від попередніх, змінених підходів до управління: заміни способів управління, які втілювались шляхом застосування владних повноважень та бюрократичних, чітко визначених процедур, на інші - такі, що реалізуються іншими важелями впливу. Поведінкова теорія в менеджменті суттєво вплинула на розвиток науки про управління та робить акцент на людському факторі в управлінні. Американка Мері Паркер Фоллетт - представниця цієї школи встановила управління (management) як “мистецтво виконувати роботу через інших людей” [18]. Анрі Файоль зазначав що «управляти – це передбачати, організовувати, розпоряджатися, узгоджувати, контролювати» [57]. Таким чином в роботі з персоналом в питаннях дотримання норм інформаційної безпеки в сучасних умовах робляться основні зусилля на інструментарій стимулювання та заохочення, в умовах воєнної агресії - почуття патріотизму, причетності до загальної справи відстоювання незалежності країни.

Проаналізуємо систему обмеження фізичного доступу до контрольованої зони. Існує велика кількість способів обмеження периметра контрольованої зони, але суть зводиться до утворення Режимного бар’єру — типовий трансмісійний, утворений одностороннім чином з метою запобігти витоку інформації поза межи державної установи. На подолання цього бар’єру й спрямовані сили і засоби зловмисників.

Наукова та промислова революції сприяли виникненню великого арсеналу засобів технічної системи охорони:

- засоби виявлення периметричного типу;

- засоби виявлення об’єктів;

- засоби, які накопичують і відображають інформацію (факту проникнення, виявлення, контроль за системою охорони, реєстрації фактів спрацювання пристрою виявлення тощо);

- засоби керування доступом (блокувальні пристрої, магнітні перепутки), пристрої механічного блокування (ворота, шлагбауми тощо);

- технічні засоби спостереження;

- технічні засоби попередження;

- технічні засоби дії (огорожі, сигнальні системи);

- інженерні споруди.

Однієї з необхідних умов підтримання достатнього рівня безпеки інформаційних ресурсі є секретне діловодство та інші складові режиму секретності у відповідності до нормативних документів. Зупинимось на цих аспектах докладніше. Документування інформації є обов’язкова складова діяльності з виконання завдань, які передбачені нормативними документами перед установою. Види, типи, порядок оформлення, необхідність підготовки документів на будь-яких видах матеріальних носіїв суворо регламентуються відповідними інструкціями, порядками тощо. В результати здійснення всіх передбачених владних процедур інформація фіксується на носіях, що дає можливість ідентифікації, підтвердження її достовірності та набуття юридичної сили. Таким чином, документ є основною формою організації інформації в здійсненні функцій державним органом. Законодавство дає визначення документу, як «зафіксована на матеріальному носії інформації з реквізитами, що дозволяють її ідентифікувати».

Умовою для збереження інформації з обмеженим доступом в документованому вигляді є дотримання вимог режиму секретності, а саме: порядок обліку (нанесення необхідних реквізитів на носій, заповнення форм обліку тощо), умови зберігання та роботи з ними. Доступ до інформації різної категорії відбувається тільки у суворій відповідності до розподілу обов’язків, закріплених за працівниками, та за рішенням керівника. Кожний факт ознайомлення з конкретним носієм інформації фіксується встановленим порядком.

Одне з основних зусиль у сфері документообігу, з огляду на питання безпеки інформації, повинно бути спрямовано на скорочення обсягу документаційного фонду, подальше проведення удосконалення уніфікованих систем документування, а також осучаснення нормативно-правових актів інструкторсько-методичного характеру та можливості їх застосування у системі електронного документообігу.

Необхідність озвучення інформації з обмеженим доступом в тому числі й за допомогою технічних засобах обумовлює створення в установі комплексів технічного захисту інформації (інформація в акустичному вигляді). Розглядає цю сферу захисту інформації потрібно зазначити наступне. Захист мовної інформації на об’єктах інформаційної діяльності включає в себе заходи, які можна поділити умовно в залежності від методу зняття інформації: захист акустичної інформації від витоку через ЗП - штучно створені канали; захист акустичної інформації від витоку технічними каналами, які можливо утворюються через акустичні, віброакустичні, а також акустоелектричні перетворення.

Специфіка завдань установи щодо проведення слідчих дій, в тому числі і негласних, передбачає проведення нарад, доповідей, обговорень посадовими особами робочих питань в конфіденційному режимі. Унеможливлення витоку інформації з обмеженим доступом в акустичному вигляді поза межи службових приміщень під час таких спілкувань може бути гарантовано тільки при умові створення та введення в експлуатацію відповідним чином комплексу технічного захисту інформації. Це передбачає цілий комплекс окремих заходів, які регламентовані нормативними документами технічного захисту інформації, в тому числі й проведення інструментального контролю. Методи захисту мовної інформації, які застосовуються при створення комплексу технічного захисту інформації поділяються на пасивні та активні.

Пасивні методи передбачають послаблення акустичних сигналів, що виникають у приміщенні, а також наслідків електроакустичних перетворень в дотичних лініях, що виникають як природним шляхом, так і в наслідок високочастотного нав'язування. Зниження рівня акустичного (мовного) сигналу здійснюється завдяки посилення звукоізоляції приміщень. Зниження інформаційних електричних сигналів в лініях і виключення (ослаблення) проходження сигналів високочастотного нав'язування в допоміжних технічних засобах здійснюється шляхом фільтрації сигналів. Активні методи – це створення маскуючих перешкод, придушення апаратів звукозапису і підслуховуючих пристроїв, а також знищення закладних пристроїв. У основі активних методів лежить використання різного типу генераторів перешкод, а також використання інших спеціальних технічних засобів, які блокують можливості зняття інформаційної складової акустичного сигналу шляхом його маскування або придушення роботи закладних пристроїв (акустичні колонки, вібровипромінювачі тощо).

Під час використовування об’єктів інформаційної діяльності з впровадженими комплексами технічного захисту інформації, обмежується доступ сторонніх осіб до цих приміщень, а також суміжних з ними. Періодично проводяться заходи інструментального контролю щодо відповідності технічних параметрів обладнання комплексу технічного захисту інформації приписам на експлуатацію, а також роботи по виявленню можливої наявності закладних пристроїв.

Дослідимо проведення робіт при необхідності впровадження комплексної системи захисту інформації (інформаційно-телекомунікаційні системи). Широке впровадження комп'ютерної техніки і телекомунікаційних технологій у забезпечення діяльності установи значно підвищує ефективність її роботи. Зворотній бік інформатизації – виникнення нових загроз інформаційній безпеці, нових способів, більш технологічно вищих здійснення злочинних намірів по відношенню до інформаційних ресурсів, які обробляються інформаційно-телекомунікаційними системами. Усунення можливих каналів витоку інформації при використані інформаційно-телекомунікаційних систем, в тому числі й технічних, є створення на таких об’єктах комплексної системи захисту інформації, які передбачають впровадження комплексу заходів щодо блокування несанкціонованого доступу користувачами та витоку технічними каналами.

Розглянемо також заходи при впроваджені комплексної системи захисту інформації, а саме:

* фізичного захисту комп’ютерних систем;
* регламентації: обігу інформації з обмеженим доступом;
* процедур резервування;
* внесення змін в склад обладнання, програмне забезпечення, складових комплексної системи захисту інформації;
* роботи персоналу і користувачів;
* заходи контролю і спостереження.

Всі заходи регламентуються вимогами документації на комплексну систему захисту інформації (проектній, експлуатаційній тощо). Тільки після погодження документації з Адміністрацією Держспецзв'язку України відбуваються роботи по монтажу та налаштуванню у відповідності до документів на комплексну систему захисту інформації параметрів засобів захисту інформації. В кожному конкретному випадку використовується свій набір інструментів в залежності від умов (ступень обмеження доступу інформації, яка обробляється, фізичних умов розташування об’єктів інформаційної діяльності, складу інформаційно-телекомунікаційних систем, кількості персоналу, завдань, які необхідно вирішувати при обробці інформації та т. ін.). До груп основних засобів захисту інформації можна віднести такі: фізичні, апаратні, програмні, апаратно-програмні, криптографічні та організаційні методи.

Як правило запобігання несанкціонованого доступу реалізується за допомогою програмних засобів захисту, які забезпечують ідентифікацію та автентифікацію персоналу, у відповідності до повноважень обмеження доступу до різних ресурсів, запис у реєстрі подій в електронному журналі, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Можливі технічні канали витоку блокується шляхом «зашумлення» етеру та ліній електроживлення, та встановлення розділових трансформаторів та фільтрів на них. Способів встановлення особистості (ідентифікації) користувачів чимало, з них три найпоширеніших способу ідентифікації: парольна, апаратна, біометрична ідентифікації. Кожний з них має свої переваги і недоліки, тому різні технології використовуються для різних умов, систем захисту . Весь період використання комплексної системи захисту інформації виконуються вимоги супроводжуючої документації на комплексну систему захисту інформації щодо порядку роботи на обладнанні, обмеження доступу персоналу на об’єктах інформаційної діяльності, проведення періодичного інструментального контролю щодо відповідності технічних параметрів обладнання технічного захисту інформації приписам на експлуатацію.

Одним з можливих інструментів запобіганню витоку інформації з обмеженим доступом при використані телекомунікаційних систем використовують криптографічні комплекси. Інформаційні системи можливо поділити на три складові: комп’ютерні програми, апаратне обладнання та мережеві комунікації з метою втілення (як систему захисту і запобігання) правил безпеки інформації. Таким чином, якщо перші дві складові інформаційно-телекомунікаційних систем є можливість убезпечити від можливості зняття інформації шляхом фізичного під’єднання (контакту), то інформацію, яку ми вимушені передавати по комунікаціям, є необхідність захищати зважаючи на таку небезпеку. В даному випадку захист інформації реалізується, як за допомогою програмних засобів, так і апаратних засобів криптографії.

Засоби комплексу захисту інформації займають окреме положення у системі технічного захисту інформації. Це пов'язано з більш суворими вимогами щодо порядку обігу як самих засобів комплексу захисту інформації так і ключових документів до них. Це передбачає ведення окремого діловодства, обліку документів та засобів комплексу захисту інформації, їх пересилки, зберігання тощо. До цієї категорії засобів, документів та роботи з ними допускається дуже вузьке коло працівників, які пройшли спеціальну підготовку.

Розголошення навіть окремих елементів системи комплексу захисту інформації може привести до витоку величезного обсягу інформації, яка не підлягає розголошенню. І якщо у випадках витоку інформації в інших складових системи захисту інформації факт буде становлений, як правило, дуже скоро, то при компрометації елементу комплексу захисту інформації факт витоку інформації з обмеженим доступом може бути встановлений тільки вже по наслідкам такого витоку.

Обов’язковою умовою коректного функціонування будь-якої системи захисту інформації є чітка регламентація дій персоналу. Одним з основних важелів підвищення ефективності впровадження заходів щодо підтримання інформаційної безпеки є підготовка та постійна робота з працівниками щодо дотримання внутрішнього режиму, встановлених правил поводження з відомостями в установі. При цьому обов'язково реалізуються наступні організаційні заходи:

* для всіх осіб, що отримують доступ до інформації з обмеженим доступом, необхідно визначити категорії допуску, коло службових питань для конкретної посадової особи, типи відомостей, до яких вона отримує доступ та її повноваження щодо неї;
* слід визначити особисту відповідальність за збереження і санкціонування доступу до кожного окремого інформаційного ресурсу;
* періодичний системний контроль за якістю дотримання правил та регламентів по захисту інформації як працівниками відповідного підрозділу установи, так й внутрішньою комісією, а також і залученням компетентних фахівців (експертів) з інших організацій (вище стоячих, профільних);
* класифікація інформації відповідно до ступенів обмеження доступу з метою диференціювати порядок поводження з нею (обігу, зберігання носіїв, охорони, знищення тощо).

Підсумовуючі зазначене можливо дійти висновку що тільки при ретельному аналізі всіх складових інформаційної діяльності установи існує можливість вибудувати адекватну систему захисту інформації.

**3.2. Розробка алгоритму дослідження стану забезпечення безпеки інформації у контексті новітніх тенденцій**

Основною метою розробки алгоритму дослідження стану забезпечення безпеки інформації в установі є визначити етапи та кроки дослідження обігу інформації з обмеженим доступом, яка представлена в будь-якому вигляді, формі (в електронному, акустичному або візуальному вигляді тощо) та місці (діловодство, виконавці, архів, електронний документообіг), виявлення можливих загроз її конфіденційності, доступності та збереження.

До загальних методів дослідження відносять наступні методи:

інформаційний аналіз,

формулярний аналіз,

метод уніфікації,

метод спостереження,

анкетування,

інтерв'ювання та опитування,

системний та

структурно-функціональний.

Один із найскладніших етапів - етап ознайомлення з функціонуванням система в цілому. У фахівця повинно сформуватися уявлення про установу як структуровану систему з елементами, що мають вертикальні і горизонтальні зв'язки, ієрархічні та трансієрархічні, прямі та зворотні. Слід пам'ятати, що “будь-яка система управління складається з низки дрібніших систем і сама є частиною більших систем”, а інформацію в цьому контексті потрібно сприймати як “форму зв'язку між головною та керованими підсистемами” [19].

На початковому етапі необхідно з'ясувати: організаційно-інформаційну взаємодію підрозділів, керівництва та виконавців; в який спосіб інформація надходить до керівника для прийняття рішень, які вона має властивості (актуальність, повнота, достовірність); як функціонують інформаційні потоки; як організовано контроль виконання розпоряджень тощо.

Дослідження передбачає вивчення загальної інформації про установу, структуру, кількість і якісний склад підрозділів, працівників, рівень технічного забезпечення (комп'ютери та оргтехніка, використання програм електронного діловодства, умови праці тощо). Надалі вивчається організаційна документація (положення про організацію та підрозділи); штатний розклад (відповідність між штатним складом та обсягом, складністю роботи); регламент організації роботи; посадові інструкції (відповідальність, компетенція кожного працівника).

Особливу увагу приділяють нормативні та методичні матеріали з регламентації питань безпеки інформації по кожному напрямку окремо (розділ 3.1). Дослідження нормативної бази дає можливість визначити необхідний й достатній рівень заходів, які потрібно здійснити. Значну роль має з’ясування маршрутів руху документів, умов проведення секретних робіт, які необхідно описати (можливо у вигляді схеми) з врахуванням моментів запобігання реалізації інформаційних небезпек. Визначити та кваліфікувати всі виявлені невідповідності між вимогами нормативними документами та існуючим станом справ. Згодом, на заключному етапі роботи це допоможе розробити необхідні запобіжні заходи, програму оптимізації діяльності в цілому, провести при необхідності перерозподіл зусиль, обов’язків й відповідальності між підрозділами, працівниками.

Як приклад вивчення діяльності державного органу з врахуванням питань забезпечення безпеки інформації пропоную проаналізувати один з напрямків діяльності ГУ ДФС в області. Функціями ГУ ДФС в області передбачається проведення досудового розслідування, в тому числі й негласних слідчих (розшукових) дій (ст. 246 глави 21 Кримінально-процесуального кодексу України). Вимоги щодо документального супроводження негласних слідчих (розшукових) дій передбачають підготовку цілої низькі документів, які містять інформацію з обмеженим доступом. Відповідно, під час поводженні з такою інформацією виникають обмеження, які визначені і в Кримінально-процесуальний кодекс України.

Досудове розслідування злочинів

ст. 215 КПК

- у формі досудового слідства,

- у формі дізнання (кримінальних проступків)

Обвинувальний акт

Внесення до Єдиного реєстру досудових розслідувань (ЄРДР)

п.1 ст. 214 КПК

Негласні слідчі (розшукові) дії

ст. 246 КПК

Пункт 2:

* відомості про правопорушення та особу, яка його вчинила, неможливо отримати в інший спосіб
* виключно у кримінальному провадженні щодо тяжких злочинів

Пункт 3:

Рішення приймає слідчий, прокурор,

слідчий суддя

Клопотання про звільнення особи від кримінальної відповідальності

Постанова про закриття кримінального провадження

За результатами досудового розслідування

Недопустимість розголошення відомостей досудового розслідування

(можливо розголошувати з дозволу слідчого, прокурора і в обсязі, в якому вони встановлюють можливим) Стаття 222 КПКУ

Відповідальність за розголошення Стаття 387 ККУ

Отримання матеріалів щодо Кримінального провадження

п.1 ст. 214 КПК

(заяви, повідомлення про вчинене кримінальне правопорушення )

**Рис. 3.3. Порядок дії посадових осіб при досудовому розслідувані**

*Джерело*: складено автором на основі Кримінально-процесуального кодексу [15].

. Загальний алгоритм дій посадових осіб під час здійснення досудового розслідування можливо відобразити блок-схемою (рисунок 3.3).

Кримінально-процесуальний кодекс України приписує чіткий алгоритм дій процесуальних осіб з визначенням документів, в тому числі й секретних, які розробляються під час досудового розслідування. Відокремлюючи з загалу тільки пункти, які є необхідними для виявлення інформаційних небезпек, можемо зазначити наступне, з зазначенням документів, які містять інформацію з обмеженим доступом

Слідчий ГУ ДФС в області на підставі повідомлення про необхідність проведення певних негласних слідчих (розшукових) дій, яке отримано від оперативного підрозділу, або за власною ініціативою приймає рішення про направлення до суду за погодження прокурора Клопотання про дозвіл на здійснення негласних слідчих (розшукових) дій. Суд після вивчення підстав приймає Ухвалу проздійснення негласної слідчої (розшукової) дії та направляє її до слідчого.

Слідчий в свою чергу передає в оперативний підрозділ Доручення на проведення певних негласних слідчих (розшукових) дій разом з Ухвалою на здійснення негласної слідчої (розшукової) дії або Постановою, якщо слідчий сам приймає рішення. Одночасно слідчим на прокурора направляється Повідомлення про проведення певних негласних слідчих (розшукових) дій листом з додатками (Ухвалою Суду (або Постановою) та Дорученням). Після проведення відповідних заходів з оперативно-розшукової діяльності працівником оперативного підрозділу направляється прокурору Протокол за результатами проведення негласних слідчих (розшукових) дії. За результатами негласних слідчих (розшукових) дії утворюються матеріальні носії секретної інформації, в тому числі й машинні (СД, DVD, flesh-носії та т.і.)).

Прокурор за результатами перевірки отриманих матеріалів приймає рішення про зняття грифу секретності з протоколу за результатами проведення негласних слідчих (розшукових) дії та направляє його в оперативний підрозділ. Після чого відбувається зняття грифу секретності з протоколу за результатами проведення негласних слідчих (розшукових) дії та долучення його до матеріалів справи. Таким чином виглядає окрема ділянка документообігу під час проведення негласних слідчих (розшукових) дії досудового слідства. Після

Повідомлення про необхідність проведення певних негласних слідчих (розшукових) дій (таємно)

Ухвалу про дозвіл на проведення негласної слідчої (розшукової) дії (таємно)

Клопотання про надання дозволу на проведення негласних слідчих (розшукових) дій (таємно)

Доручення на проведення певних негласних слідчих (розшукових) дій (таємно) разом з Ухвалою про дозвіл на проведення негласної слідчої (розшукової) дії (таємно) або Постановою

 (таємно)

Погоджує

Клопотання на проведення негласної слідчої (розшукової) дії (таємно)

Одночасно

Повідомлення про проведення певних негласних слідчих (розшукових) дій (Т) листом з додатками (Ухвалою Суду (або Постановою) та Дорученням

рішення про зняття грифу секретності з протоколу за результатами проведення негласних слідчих (розшукових) дії (таємно

 Протокол за результатами проведення негласних слідчих (розшукових) дії (таємно) (за результатами НСРД утворюються МНСІ, в тому числі й машинні (СD, DVD, flesh-носії та т.і.))

 після зняття грифу секретності до прокурора протокол за результатами проведення негласної слідчої (розшукової) дії

Оперативний підрозділ

Слідчий підрозділ

Прокуратура

Суд

**Рис. 3.4. Обіг інформації (документів) під час здійснення слідчих досудового розслідування**

*Джерело:* складено автором на основі Кримінально-процесуального кодексу України [15]

кожної процесуальної дії відбувається розробка відповідного документу з дотриманням умов, які визначені нормативними документами з режиму секретності, реєстрація їх у визначених формах обліку (електронних реєстрах), та подальші маніпуляції згідно Кримінально-процесуального кодексу України.

Порядок обігу інформації (документів) можливо відобразити у вигляді схеми (рисунок 3.4).

При узагальненні вимог нормативних документів, частина яких має закритий для загалу характер, зробимо спробу визначити основні питання для дослідження (контролю) стану інформаційної безпеки установи окремо по кожному напрямку окремо: з режиму секретності та технічного захисту інформації.

Під час дослідження стану режиму секретності необхідно проаналізувати наступні питання:

* порядок зберігання матеріальні носії секретної інформації (розташування, облаштування, обмеження доступ);
* умови роботи з матеріальними носіями секретної інформації виконавцями (місця для роботи, наявність необхідних облаштунків);
* наявність відповідних внутрішніх регламентуючих документів, щодо запобіганню порушенню режиму секретності, та доведення їх до виконавців;
* дотримання вимог по доступу до інформації з обмеженим доступом (МНСІ, проведення закритих нарад тощо) (погодження з органами Служби безпеки України, зазначення у функціональних обов’язках, рішення керівництва та т.ін.);
* порядок надання грифів секретності, ступенів обмеження доступу матеріальних носіїв секретної інформації (засекречування, розсекречування, періодичний їх перегляд, проведення експертної оцінки інформації);
* ведення секретного та службового діловодства (номенклатура справ, книги та журнали обліку, реєстрація, отримання, відправки, тимчасової передачі, складання та оформлення матеріальних носіїв секретної інформації);
* архівне зберігання (оформлення номенклатурних справ, передача до архіву, умови зберігання та роботи з документами);
* процедура знищення матеріальних носіїв секретної інформації;
* повсякденний контроль за дотриманням поводження з матеріальними носіями секретної інформації та інших секретних робіт;
* підготовка документів та інших матеріальних носіїв секретної інформації з використанням інформаційно-телекомунікаційних систем;
* порядок забезпечення режиму секретності під час міжнародного співробітництва.

Розглянемо окремо питання, які підлягають контролю з технічного захисту інформації. Під час контролю стану технічного захисту інформації пропоную поділити дослідження на окремі етапи (створення та експлуатації) щодо комплексів технічного захисту інформації на об’єктах інформаційної діяльності, де озвучується та/або обробляється технічними засобами секретна інформації, та комплексних систем захисту інформації автоматизованих систем класу «1» призначених для обробки інформації з обмеженим доступом.

Алгоритм проведення дослідження фактичного стану технічного захисту інформації на об’єкті інформаційної діяльності, які створені для озвучення чи обробки технічними засобами інформація з обмеженим доступом пропоную формалізувати у табличному вигляді (таблиці 3.2, 3.3, 3.4, 3.5).

*Табл. 3.2*

**Питання перевірка на об’єкті інформаційної діяльності, де озвучується та/або обробляється технічними засобами секретна інформації**

**(проектна, експлуатаційна та інша технічна документація)**

**(на етапі створення комплексу технічного захисту інформації)**

|  |  |
| --- | --- |
| Найменування питання | Короткий зміст перевірки |
| Встановлення категорії об’єктів інформаційної діяльності (НД ТЗІ 1.6-006-2015). | - відомості про розташування об’єктів інформаційної діяльності;- визначення категорії об’єкту та умов розташування;- акт категоріювання. |
| Модель загроз для інформації (НД ТЗІ 1.6-003-2004). | - наявність Моделі загроз;- відповідність даних Моделі загроз та Акту обстеження;- ситуаційний план; - повнота викладених загроз відповідно до вихідних даних за результатами спеціальних досліджень. |
| Відповідність розміщення схемам у Моделі загроз та в Паспорті на комплекс технічного захисту інформації. | * будівлі, де розташований об’єкт інформаційної діяльності;
* об’єктів навколо;
* суміжних приміщень;
* складу та розміщення технічних засобів.
 |
| Перевірка відповідності складу та розміщення комплексу технічного захисту. | шляхом порівняння фактичного розміщення та складу з відомостями зазначеними в Паспорті на комплекс технічного захисту інформації. |
| Перевірка коректності визначених вимог до захисту інформації від витоку технічними каналами. | шляхом порівняння вимог ТЗ до захисту інформації від витоку технічними каналами і визначених загроз для інформації у Моделі загроз. |
| Перевірка виконання етапів створення комплексу технічного захисту інформації. | відповідність з нормативно-правовими актами та нормативними документами технічного захисту інформації відповідно до вимог НД ТЗІ 3.6-003-2016. |
|  | Перевіряється наявність діючих сертифікатів відповідності (експертних висновків) до Переліку таких засобів, якій розміщується на офіційному веб-сайті ДССЗЗІ України. |

*Джерело:* складено автором на основі нормативних документів у галузі технічного захисту інформації [22, 23, 24].

*Табл. 3.3*

**Питання перевірка на об’єкті інформаційної діяльності, де озвучується та/або обробляється технічними засобами секретна інформації**

**(проектна, експлуатаційна та інша технічна документація)**

**(на етапі функціонування комплексу технічного захисту інформації)**

|  |  |
| --- | --- |
| Найменування питання | Короткий зміст перевірки |
| Встановлення категорії об’єктів інформаційної діяльності. | - відомості про розташування об’єктів інформаційної діяльності;- термін дії Акту категоріювання;- актуальність відомостей наведених у Акті категоріювання. |
| Модель загроз для інформації (НД ТЗІ 1.6-003-2004). | - актуальність відомостей у Моделі загроз та Акті обстеження;- наявність в ситуаційному плані всіх факторів, які можуть сприяти виникненню витоку інформації технічними каналами; - повнота викладених загроз для інформації за результатами спецдосліджень;- склад та розміщення основних технічних засобів, допоміжним технічних засобів, транзитних комунікацій |
| Відповідність складу та розміщення комплексу технічного захисту інформації (засобів технічного захисту інформації). | шляхом порівняння фактичного розміщення та складу з відомостями зазначеними в Паспорті на комплекс технічного захисту інформації. |
| Відомості у Паспорті на комплекс технічного захисту інформації про проведення робіт.  | - атестація комплексу технічного захисту інформації- інструментальний контроль;- роботи з виявлення закладних пристроїв на об’єкті інформаційної діяльності тощо. |
| Наявність сертифікатів відповідності або експертних висновків на засоби технічного захисту інформації. | Термін експлуатації засобів технічного захисту інформації може продовжуватися виробником або за результатами державної експертизи. Кожен раз - не більш ніж на 3 роки |

*Джерело:* складено автором на основі нормативних документів у галузі технічного захисту інформації [22, 23, 24].

*Табл. 3.4*

**Питання перевірка автоматизованих систем класу «1» призначених для обробки інформації з обмеженим доступом**

 **(на етапі створення комплексу технічного захисту інформації)**

|  |  |
| --- | --- |
| Найменування питання | Короткий зміст перевірки |
| Встановлення категорії об’єкту інформаційної діяльності(НД ТЗІ 1.6-005-2013). | - правильність категорії об’єкту;- наявність та правильність відпрацювання акта категоріювання. |
| Наявність, чинність проектної, експлуатаційної та іншої технічної документації на автоматизовану систему класу «1». | відповідність переліку документів наведеному у додатку до Порядку організації проведення експертних випробувань та оцінка відповідності |
| Призначення адміністраторів. | наявність та актуальність наказу. |
| Порядок введення в експлуатацію автоматизованої системи. | наявність та актуальність наказу, надання дозволу на обробку інформації в автоматизованій системі. |
| Комплекс технічного захисту інформації  | склад та відповідність документації на комплексну систему захисту інформації в класу «1» |
| Атестат відповідності та Експертного висновку  | перевірка відомостей щодо чинності та актуальності |
| Основні технічні засоби, допоміжні технічні засоби, засоби захисту інформації та програмне забезпечення.  | перевірка фактичного складу та відповідності Формуляру на автоматизовану систему. |
| Випробування автоматизованої системи.  | наявності відомостей зазначених у Формулярі на автоматизовану систему. |
| Відповідальні особи за автоматизовану систему. | наявності відомостей зазначених у Формулярі на автоматизовану систему. |
| Налаштування комплексу засобів захисту. | Перевірка відповідності параметрів документації та нормативної документації. |
| Порядок застосування комплексу засобів захисту.  | Перевірка відповідності параметрів документації та нормативної документації. |
| Вибіркова перевірка відповідності записів в журналах обліку режиму секретності (службового діловодства) та реквізитів документа журналу захисту комплексу засобів захисту (журналу обліку роботи користувачів, небезпечних подій тощо). |
| Вибіркова перевірка фактів обробки інформації, що підлягає захисту, в автоматизованій системі, які не призначені для обробки такої інформації. |

*Джерело*: складено автором на основі нормативних документів у галузі технічного захисту інформації [22, 23, 24].

*Табл. 3.5*

**Питання перевірка автоматизованих систем класу «1» призначених для обробки інформації з обмеженим доступом**

 **(на етапі функціонування комплексу технічного захисту інформації)**

|  |  |
| --- | --- |
| Найменування питання | Короткий зміст перевірки |
| Правильність категорії об’єкту інформаційної діяльності(НД ТЗІ 1.6-005-2013). | - термін дії Акту категоріювання;- актуальність відомостей наведених у Акті категоріювання на час проведення перевірки. |
| Наявність, чинність проектної, експлуатаційної та іншої технічної документації на автоматизовану систему класу «1». | відповідність переліку документів наведеному у додатку до Порядку організації проведення експертних випробувань та оцінка відповідності |
| Призначення адміністраторів. | наявність та актуальність наказу. |
| Порядок введення в експлуатацію автоматизованої системи. | наявність та актуальність наказу, надання дозволу на обробку інформації в автоматизованій системі. |
| Комплекс технічного захисту інформації  | склад та відповідність документації на комплексну систему захисту інформації в класу «1» |
| Атестат відповідності та Експертного висновку  | перевірка відомостей щодо чинності та актуальності |
| Основні технічні засоби, допоміжні технічні засоби, засоби захисту інформації та програмне забезпечення.  | перевірка фактичного складу та відповідності Формуляру на автоматизовану систему. |
| Супроводження експлуатації автоматизованої системи. | перевірка наявності відомостей у розділах Формуляру на автоматизовану систему. |
| Працездатність комплексу засобів захисту. | перевірка працездатності технічних засобів, які входять до комплексу засобів захисту. |
| Вибіркова перевірка відповідності записів в журналах обліку режиму секретності (службового діловодства) та реквізитів документа журналу захисту комплексу засобів захисту (журналу обліку роботи користувачів, небезпечних подій тощо). |
| Вибіркова перевірка фактів обробки інформації, що підлягає захисту, в автоматизованій системі, які не призначені для обробки такої інформації. |

*Джерело:* складено автором на основі нормативних документів у галузі технічного захисту інформації [22, 23, 24].

Враховуючі вище зазначене зауважимо, що узагальнення у вигляді рекомендацій вимог нормативних документів та процесів, пов’язані з проведенням контролю стану інформаційної безпеки, дає змогу підвищити ефективність роботи працівників підрозділів, які відповідальні в установі за захист інформації.

**Висновки до розділу 3**

Сучасні умови діяльності системи державного управління потребують оперативного реагування на зміни, фактори впливу (внутрішнього та зовнішнього) з метою, в тому числі, й підтримки відповідного рівня інформаційної безпеки установи.

Організація контролю за станом безпеки інформації (режиму секретності та технічного захисту інформації) є необхідним елементом для успішного подолання інформаційних загроз сьогодення та процесом багатофакторним та багатоступеневим, якій пов’язаний із нормативною та законодавчою базою.

Це зумовлює необхідність узагальнення підходів до питань здійснення контролю стану інформаційної безпеки у вигляді формалізованих етапів – рекомендацій, методики.

Проведення контрольних заходів з врахуванням запропонованих рекомендацій дає змогу забезпечити проведення зазначених робіт більш ефективно та якісно посадовими особами підрозділів захисту інформації.

Досягнути необхідного рівня захищеності можливо тільки за рахунок певних принципів захисту інформації, до яких належіть комплексне використання існуючих методів і засобів захисту, безперервну реалізацію заходів із захисту інформації, необхідність та достатність комплексу засобів та заходів, адекватність витрат на захист вартості можливої шкоди внаслідок реалізації загроз [17].

Разом з цим необхідно підкреслити, що при вирішенні питань охорони держаної таємниці економічність фінансування проведення заходів не є пріоритетним.

**ВИСНОВКИ ТА ПРОПОЗИЦІЇ**

 Сьогоднішні умови розвитку цивілізації не можливо уявити без постійного напрацювання, обміну, зберігання великих масивів інформації. Наявність необхідної інформації та правильне її використання практично спроможна вирішити будь-які проблеми. Велику роль мають аспекти обігу інформації у питаннях підтримки стабільності та розвитку всіх сфер суспільства. Особливе місце інформаційна складова займає у публічному управлінні, системі державної влади. Як й будь-яка важлива сфера суспільного життя інформаційна постійно перебуває під увагою держави. Це підтверджується масивом законодавчих актів, які встановлюють правила обігу, використання, поширення різних відомостей. Встановлюються також й обмеження різних дій з інформацією, які можуть привести до нанесення шкоди особі, організації, суспільству, державі. Окреме місце займають питання безпеки при використанні інформації. Виклики сьогодення, в тому числі й в інформаційній сфері, вимагають підтримки захисту інформації в органах державної влади на достатньому рівні.

У кваліфікаційній роботі  проведено теоретичне узагальнення та розроблено підходи до організації функціонування системи захисту інформації, призначення служби захисту інформації у державних органах; обґрунтовано теоретичні та організаційно-правові засади побудови системи захисту інформації; проаналізовано сучасний стан та проблеми системи забезпечення безпеки інформації в органах ДФС України; запропоновано шляхи удосконалення захисту інформації в Головному управління ДФС в Тернопільській області

У відповідності до встановленої мети роботи та визначених завдань було зроблено наступне.

1. У результаті системного аналізу робіт вітчизняних і зарубіжних науковців, нормативно-правових документів та інших джерел проведено розкриття теоретичних основ забезпечення безпеки інформаційної діяльності в структурі загальної діяльності установи в цілому. Визначено, що питання захисту інформаційних ресурсів державних органів є актуальним у світлі проведення цифрової трансформації суспільства. Акцентована увага на проблемі постійних змін у галузі інформаційної безпеки на сучасному етапі. За результатами проведеного аналізу практичних заходів захисту інформації в держаних установах, в тому числі в органах ДФС Україні підтверджено, що відбувається зростання кількості варіантів загроз щодо інформації з обмеженим доступом, яка перебуває у власності державних установ. Окрім того, підкреслено на зростанні в умовах економічної нестабільності людського фактора у питаннях запобігання витоку інформації. Тому, на нашу думку при реформування державної служби необхідно враховувати фактори постійних загроз з боку зловмисників щодо інформаційних ресурсів держави. Необхідно зауважити, що державна служба у сучасних умовах в сфері інформаційної безпеки відстає від приватного сектору, в якому знаходяться більш підготовлені фахівці та більші фінансові ресурси. Це має спонукати до активізації заходів щодо підтримки постійного зв’язку державних органів з науковим середовищем.
2. Після узагальнення зарубіжного та вітчизняних наукових матеріалів проведена класифікацію потенційних загроз інформації, яка використовується в установах системи державної влади. Досліджені питання обігу матеріальних носіїв інформації з обмеженим доступом. В роботі було підкреслено, що в державній органах захисту підлягає вся інформація, яка є власністю держави. Проведений аналіз потенційних загроз інформаційній безпеці. Докладніше розкрити існуючі небезпеки для властивостей інформації, які розглядаються при вирішені питань її захисту. У роботі з’ясовані можливі варіанти порушення безпеки інформації та основні напрямки діяльності щодо їх запобігання. У цьому контексті акцентовано увагу на існуванні понять політики безпеки» (при використання інформаційно-телекомунікаційної системи для обробки інформації з обмеженим доступом) та режиму секретності (для обігу секретної інформації поза інформаційно-телекомунікаційної системи). Охарактеризовано процеси утворення каналів витоку інформації з окремим висвітленням основним фізичних каналів.
3. Приділено увагу здійсненню моніторингу рівня інформаційної безпеки. Обов’язковою умовою вирішення цього питання та підтримання необхідного рівня захисту інформації є наявність окремих підрозділів (окремих посадових осіб), за якими закріплені відповідні функції з режиму секретності та технічного захисту інформації, а також утвореними у підрозділах службами захисту інформації в інформаційно-телекомунікаційній системі. Проведений аналіз законодавчого підґрунтя діяльності таких підрозділів, їхній статус, завдання, функції. Саме робота підрозділу з функціями управління системою захисту інформації є базових елементів цієї системи. У цьому контексті акцентовано увагу на діяльність такого підрозділу, зокрема у питаннях моніторингу та контролю стану інформаційної безпеки. Вагома роль при цьому належить виконавчий дисципліні та корпоративній культурі, яка безпосередньо впливає на дотримання всіх встановлених правил та вимог поводження з інформаційними ресурсами. Значно підвищується увага до ролі особистості в роботі державних органів. Кроком до вирішення проблем підтримання рівня інформаційної безпеки установи буде постійна робота з персоналом, їх підготовка та контроль за всіма маніпуляціями щодо інформації з обмеженим доступом.
4. У процесі дослідження розглянуто підходи до проведення вивчення інформаційної діяльності та розробки методики проведення аналізу та контролю за станом безпеки інформації в установі. Спираючись на положення Кримінально-процесуальний кодекс України складений у вигляді блок-схеми алгоритм дій посадових осіб органу Державної фіскальної служби під час здійснення досудового розслідування, а саме негласних слідчих (розшукових) дій. Після проведеного аналізу низькі законодавчих, нормативних та інших керівних документів щодо захисту інформації, необхідно дійти висновку, що організація контролю у сфері безпеки інформації є необхідним елементом для успішного виконання функцій державного органу та багатофакторним, багатоступеневим процесом, що регламентується багатьма керівними документами і залежить від внутрішніх і зовнішніх чинників, а також напряму пов’язаний із законодавчою базою.
5. В роботі робиться один з висновків, що захист інформації неможливо регламентувати за єдиним шаблоном через різноманітність в кожній організації своїх існуючих інформаційних процесів, інформаційно-телекомунікаційних систем та видів інформації, що обробляється. Конкретні заходи визначаються виробничими, організаційними, фінансовими і іншими потребами та можливостями установи, обсягом інформації з обмеженим доступом та її пріоритетності.

Існує можливість сформулювати тільки загальні підходи:

проектування, впровадження та супроводження системи захисту інформації є багатоскладовою, відповідальною справою, яку повинні проводити підготовлені фахівці;

не потрібно намагатись створити абсолютно надійний захист — таке практично неможливо. Система захисту має бути достатньою, ефективною та керованою. Ефективність системи захисту інформації полягає у здатністю адекватно реагувати на всі можливі загрози;

 захист інформації повинен носити комплексний характер, та включати різні напрямки та засоби;

 систему захисту необхідно будувати, виходячи з основної існуючої в будь кому випадку загрози, яку становлять співробітники установи.

За результатами узагальнень нормативної бази, комплексного аналізу організаційно-правових засад та практичної роботи розроблені методичні рекомендації щодо аналізу та контролю за станом режиму секретності та технічного захисту інформації, яка містить у собі основні питання дослідження стану захисту інформації. Методика враховує вимоги нормативних документів, вплив зовнішніх та внутрішніх чинників. Таким чином, розробка методик аналізу та контролю за станом режиму секретності та технічного захисту інформації, які віддзеркалюють вимоги нормативних документів, дає можливість підвищення ефективності діяльності персоналу, якій проводять заходи з питань захисту інформації.

Отже, процеси, які відбуваються на сучасному етапі розвитку держави, проведення діджиталізації суспільства вимагають істотних змін у підходах щодо методів управління системою захисту інформації в державних органах. Державний орган є один з основних елементів підґрунтя держави та її інформаційної безпеки. Тому необхідно зробити висновок, що тільки покращуючи якість організації процесів управління, в тому числі й в питання захисту інформації, можливо забезпечити належний рівень безпеки незалежної України

**Список використаних джерел**

1. Антонюк А.А., Волощук А.Г., Суслов В.Ю., Ткач А.В. Что такое Оранжевая книга? (Из истории компьютерной безопасности) // Безопасность информации. - №2. - 1996.

2. Антонюк А.А., Заславская Е.А., Лащевский В.И. Некоторые вопросы разработки политики безопасности информации // Защита информации: Сб. науч. тр. -К.: КМУГА, 1999. - 188 с.

3**.**  Афанасьев В.Г. Социальная информация и управление обществом. – М., . Госкомиздат.1975. 125с.

4. Варенко В. М., Братусь І. В., Дорошенко В. С., Смольніков Ю. Б., Юрченко В. О. Системний аналіз інформаційних процесів: Навч. посіб. / К.: Університет «Україна», 2013. 203 с. URL:http://nbuvіap.gov.ua/іmages/nak\_mon\_partnerіv/SA.pdf (дата звернення: 22.06.2021)

5. Винер Н. Кибернетика. /Н. Винер. – М. Госкомиздат.1958. 220с.

6. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — 98 с.)

7. Галатенко В.А. Информационная безопасность: практический подход. -М.: Наука, 1998.-301 с.

8. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

9. Глушков В. М. Кибернетика. Вопросы теории и практики / В. М. Глушков. – М. : Наука, 1986. – 488 с.

10. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99.- К. ДСТСЗІ СБ України, 1999- 16с.

11. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл

12. Конституція України від 28.06.1996 № 254к/96-ВР. URL: http://zakon2.rada.gov.ua/laws/show/1264-12 (дата звернення 16.05.2021).

13. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник для студ. вищих навч. закл. К.: Кондор, 2004. 384 с.

14. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. ― Х., 2004. ― 42 c.

15. Кримінально-процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

16. Ларін М.В. Управление документацией в организациях: проблеми истории и методология. М., 2000, 413 с.) (дата звернення 16.08.2021).

17. Ленков С.В., Перегудов Д.А., Хорошко В.А., Методы и средства защиты информации/ под. ред. В.А.Хорошко. – К.: Арий, 2008. – Том І. Несанкционированное получение информации, – 464 с.

18. Mary P. Follett. Creatіng Democracy, Transformіng Management, Tonn, Joan C., New Haven: Yale Unіversіty Press, 2003. 366 p

19. Макарский Ю.И. Потоки информации на предприятии и ее обработка. -М.:Экономика,1957. -43 с. ].

20. Нарис історії охорони державної таємниці в Україні: Монографія / В.П. Ворожко, Б.В. Бернадський, О.В. Бортвінкін / Наукове видання. – К., 2012. – 188 с.

21. НД ТЗІ 1.1-002-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення 15.07.2021).

22. НД ТЗІ 1.1-005-07 “Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення”. URL:https://tzi.com.ua/downloads/1.1-005-07.pdf (дата звернення 21.08.2021).

23. НД ТЗІ 1.4-001-2000 “Типове положення про службу захисту інформації в автоматизованій системі”. URL:https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення 11.09.2021).

24. НД ТЗІ 2.1-002-07 “Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення”. URL:https://tzi.com.ua/downloads/2.1-002-07.pdf (дата звернення 25.07.2021).

25. НД ТЗІ 2.5-008-02 “Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”.URL:https://tzi.com.ua/downloads/2.5-008-02.pdf (дата звернення 25.09.2021).

26. НД ТЗІ 2.5-010-03 “Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/2.5-010-03.pdf (дата звернення 22.09.2021).

27. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення 18.09.2021).

28. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/2.5-005-99.pdf (дата звернення 28.07.2021).

29. НД ТЗІ 2.7-010-09 “Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/2.7-010-09.pdf (дата звернення 11.09.2021).

30. НД ТЗІ 3.1-001-07 “Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи”. URL:https://tzi.com.ua/downloads/3.1-001-07.pdf (дата звернення 12.07.2021).

31. НД ТЗІ 3.3-001-07 “Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації”. URL:https://tzi.com.ua/downloads/3.3-001-07.pdf (дата звернення 28.07.2021).

32. НД ТЗІ “Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу”. URL:https://tzi.com.ua/downloads/3.6-001-2000.pdf (дата звернення 18.09.2021).

33. НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі”. URL:https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення 16.07.2021).

34. НД ТЗІ 3.7-003 -2005 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”. URL:https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення 16.05.2021).

35. НД ТЗІ 2.2.011-2015 Норми ефективності захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень ­ Київ,: ДССЗ, 2015. ­ 15с

36. Основи інформаційної безпеки та технічного захисту інформації, Рибальський О.В., Хахановський В.Г., Кудінов В.А., посібник, Національна академія внутрішніх справ МВС України, УДК 681.518 (075.8), 2012, -104с.

37. Положення про Державну фіскальну службу України (затверджено постановою Кабінету Міністрів України від 21 травня 2014 р. № 236) <https://zakon.rada.gov.ua/laws/show/236-2014-%D0%BF#Text> (дата звернення: 22.09. 2021).

38. Про інформацію: Закон України від 02.10.1992 № 2657-XІІ. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення 15.05.2021).

39. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-ІV. URL: <https://zakon.rada.gov.ua/laws/show/964-15#Text> (дата звернення 16.05.2021).

40. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text> (дата звернення 15.05.2021).

41. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015. URL. http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення 17.05.2021).

42. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р. URL: h1ttps://www.kmu.gov.ua/npas/246420577 (дата звернення 16.05.2021).

43. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12.01.2015 № 5/2015. URL. <http://zakon5.rada.gov.ua/laws/show/5/2015> (дата звернення 16.05.2021).

44. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015. URL. http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення 17.05.2021).

45. Про рішення Ради національної безпеки і оборони України від 27  січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL. http://zakon2.rada.gov.ua/laws/show/96/2016 (дата звернення 17.05.2021).

46. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України". Указ Президента України від 01.05.2014 № 449/2014. URL. ([https://www.presіdent.gov.ua/documents/4492014-17157](https://www.president.gov.ua/documents/4492014-17157)) (дата звернення 17.05.2021).

47. Про державну таємницю. Закон України від 21.01.1994 № 3855-XІІURL:https://zakon.rada.gov.ua/laws/show/3855-12?fіnd=1&text=%D0%B2%D0%B8%D1%89%D0%B5%D1%81%D1%82#w1\_1 (дата звернення: 21.08.2021).

48. Про Концепцію (основи державної політики) національної безпеки України, Постанова Верховної Ради України від 16 січня 1997 року N 3/97-ВР URL: https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80#Text (дата звернення 15.05.2021).

49. Про затвердження Концепції технічного захисту інформації в Україні. Постанова Кабінету Міністрів України від 08.10.1997 року № 1126 URL: <https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text> (дата звернення 24.08.2021).

50. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова Кабінету Міністрів України від 13.03.2002 р. N 281 URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF#Text (дата звернення 28.09.2021).

51. Про захист інформації в інформаційно-телекомунікаційних системах. Законом України (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286)

52. Положення про Державну фіскальну службу України (Постанова Кабінету Міністрів України від 21 травня 2014 р. № 236). URL: <https://zakon.rada.gov.ua/laws/show/236-2014-%D0%BF#Text> (дата звернення 27.09.2021).

53. Савченко П.В. «Захист інформації від витоку по технічним каналах». [Електронний ресурс] – режим доступу­ <http://refdb.ru/look/1176205.html>. (дата звернення 18.07.2021)

54. M. Sіponen, "Fіve dіmensіons of іnfor-matіon securіty awareness", Computers and Socіety, pp. 24-29, 2001.

55. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок ­ Київ,: ДСТЗІ, 1995,­ 26с.

56. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1—003—99.— К.: ДСТС31 СБ України, 1999.- 26 с

57. Fayol, Henrі (1916), Admіnіstratіon іndustrіelle et générale; prévoyance, organіsatіon, commandement, coordіnatіon, controle, Parіs, H. Dunod et E. Pіnat. – Режим доступу : http://www.worldcat.org/ (дата звернення: 22.09. 2021)

58. Шенон К. Работы по теории информации и кибернетике. М. : Изд-во иностр. лит., 1963. 825 с.