

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

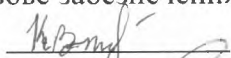
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
КАФЕДРА ФІНАНСОВОГО ТА ПОДАТКОВОГО ПРАВА

ВИПУСКНА РОБОТА

на тему: Правові аспекти захисту податкової інформації

Здобувача вищої освіти II рівня, II курсу, ПМФ-23-1 групи,
спеціальності 081 «Право»

освітня програма «Правове забезпечення фінансової безпеки держави»


(підпис)

Кузьмич Владислав Миколайович
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Касьяненко Любов Михайлівна, д.ю.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

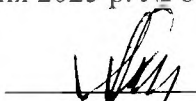
Керівник освітньо-професійної
програми


(підпис)

Білоус Віктор Тарасович, д.ю.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Допущено до захисту за рішенням кафедри фінансового та податкового права
протокол від «09» січня 2025 р. № 8.

Завідувач кафедри


(підпис)

Глух Марина Василівна, к.ю.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Ірпінь – 2025

Реєстрація № 7 27.01.2025р. [Signature]
(дата) (підпис відповідальної особи)

Результати перевірки до захисту 04.01.2025р. [Signature]
(до захисту, на доопрацювання) (дата) (підпис)

Результат захисту Вірнено 11.02.2025р. [Signature]
(оцінка) (дата) (підпис)

Голова комісії: [Signature] М.В. Кармаліта
(підпис) (ініціали, прізвище)

Члени комісії: [Signature] М.В. Глух
(підпис) (ініціали, прізвище)

[Signature] В.Т. Білоус
(підпис) (ініціали, прізвище)

[Signature] А.В. Гарбінська-Руденко
(підпис) (ініціали, прізвище)

БЛАНК ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.П.: голови комісії членів комісії секретаря, (підписи)
ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1.Доповідь	від 0 до 10	10		1. М. М. М. 2. А. А. А. 3. В. В. В. 4. Б. Б. Б. 5. С. С. С.
2. Роздатковий матеріал	від 0 до 5	5		
3. Знання теоретичного та практичного матеріалу, вміння відповідати на запитання	від 0 до 25	25		
5. Апробація (участь у конференціях)	від 0 до 10			
РАЗОМ БАЛІВ	від 0 до 50	50		
ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	від 0 до 100	90		

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.П.: голови, членів комісії, секретаря, (підпис)
90	A	Відмінно	11.02.25	1. М. М. М. 2. А. А. А. 3. В. В. В. 4. Б. Б. Б. 5. С. С. С.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ ПРАВОВИХ АСПЕКТІВ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ	12
1.1 Поняття податкової інформації та правові засади конфіденційності, безпека податкової інформації.....	12
1.2. Законодавство щодо захисту податкової інформації, національна та міжнародна практика.....	19
РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ПОДАТКОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ ПРАКТИЧНИЙ АНАЛІЗ СУЧАСНИХ ПРОБЛЕМ ТА ВИКЛИКІВ У ЗАХИСТІ ПОДАТКОВОЇ ІНФОРМАЦІЇ	24
2.1. Види правового режиму податкової інформації.....	24
2.2. Випадки порушення захисту податкової інформації.....	32
2.3.Способи попередження порушень та зловживань у сфері захисту податкової інформації.....	38
РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ	45
3.1. Технологічні засоби захисту та організаційні заходи для запобігання не санкційованому доступу.....	45
3.2. Інноваційні технології та розробки сучасного забезпечення для захисту податкової інформації.....	56
ВИСНОВКИ	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	70

ВСТУП

Одним із ключових елементів ефективного функціонування податкової системи є забезпечення захисту податкової інформації. У сучасних умовах глобалізації, цифровізації та постійного зростання обсягів інформаційних потоків значення цієї проблеми суттєво зростає. Впровадження сучасних технологій, зокрема автоматизованих систем обробки даних, хмарних рішень та блокчейн-технологій, створює нові можливості для підвищення ефективності роботи податкових органів, але водночас і нові виклики для забезпечення безпеки даних.

Актуальність теми. Захист податкової інформації є надзвичайно актуальним для України, особливо в умовах війни, яка триває другий рік. У сучасному світі податкова інформація має стратегічне значення, адже вона є основою для формування державного бюджету, забезпечення фінансування оборонного сектора, соціальних програм та інших ключових функцій держави. Під час війни ефективне адміністрування податків та надійний захист відповідної інформації стають критичними для збереження фінансової стабільності країни, а також забезпечення прозорості у використанні ресурсів.

У контексті прагнення України стати повноправним членом Європейського Союзу тема захищеності податкової інформації набуває нового значення. Європейські стандарти захисту даних, зокрема Загальний регламент про захист даних (GDPR), вимагають високого рівня правового, організаційного та технічного забезпечення конфіденційності й безпеки інформації. Впровадження цих стандартів у національну податкову систему є важливим кроком на шляху до євроінтеграції. Це забезпечує гармонізацію правових норм із законодавством ЄС, зміцнює довіру європейських партнерів і сприяє залученню іноземних інвестицій, які є необхідними для відновлення економіки після завершення війни.

Окрім того, в умовах гібридної війни питання інформаційної безпеки набуває нових викликів. Податкова інформація, яка містить чутливі дані про економічний стан підприємств, обсяги державних доходів, податкові

надходження та фінансові резерви, може стати об'єктом кібератак з боку противника. Збереження цієї інформації у безпеці є важливим не лише для забезпечення стабільної роботи податкових органів, але й для уникнення ризиків витоку даних, які можуть бути використані для дестабілізації економіки або підриву довіри до державних інституцій.

Таким чином, дослідження правових аспектів захисту податкової інформації є актуальним у кількох вимірах: воно має важливе практичне значення для забезпечення економічної безпеки держави, відповідає стратегічним завданням інтеграції України до ЄС та сприяє підвищенню ефективності управління державними фінансами в умовах сучасних викликів.

Мета і завдання дослідження. Метою дослідження є визначення теоретичних засад і розробка практичних рекомендацій щодо правового захисту податкової інформації.

Завдання роботи включають аналіз понять і правових засад конфіденційності, вивчення законодавчої практики, класифікацію правових режимів, виявлення типових порушень і способів їх попередження, а також оцінку сучасних технологій захисту податкової інформації.

Стан і ступінь розробки проблеми в спеціальній літературі. В основу дослідження правового режиму податкової інформації в Україні покладені наукові праці таких учених, як: В. Л. Андрущенко, І. В. Арістової, В. Т. Білоуса, О. О. Бригінця, М. М. Бліхар, Р. О. Гаврилюк, М. В. Гуцалюка, Д. О. Гетманцева, Е. С. Дмитренко, Т. О. Коломоєць, А. І. Крисоватого, М. П. Кучерявенка, Н. А. Литвин, П. Є. Матвієнко, О. В. Машенко, А. М. Новицького, Н. Б. Новицької, В. О. Рядінської, В. І. Теремецького, В. С. Цимбалюка, та ін., а також зарубіжні дослідники, що аналізували міжнародні стандарти, зокрема GDPR. Основу роботи становить чинне законодавство України та методологічні підходи до інформаційної безпеки.

Об'єктом дослідження є правові відносини, що виникають у процесі захисту податкової інформації в умовах сучасної правової, економічної та технологічної реальності.

Предметом дослідження є суспільні відносини та правові механізми, принципи та інструменти забезпечення захисту податкової інформації. Це включає аналіз нормативно-правової бази України та міжнародного законодавства, підходів до регулювання доступу, обробки та зберігання податкових даних, а також дослідження сучасних технологій, що використовуються для запобігання несанкціонованому доступу і забезпечення конфіденційності податкової інформації.

Методи дослідження. У дослідженні застосовано комплекс методів, що відповідають його меті та завданням. Зокрема, використано історико-правовий метод для аналізу розвитку правового регулювання захисту податкової інформації, порівняльно-правовий метод — для вивчення вітчизняної та міжнародної законодавчої практики. Системний підхід дозволив визначити місце податкової інформації в загальній інформаційній системі держави, а метод аналізу і синтезу — дослідити види правових режимів податкової інформації та технологічні засоби її захисту. Практичну складову забезпечено емпіричним методом, спрямованим на вивчення реальних випадків порушень і їх наслідків.

База досліджень. Базою дослідження виступили установи та фінансові інститути, що діють у сфері фінансового адміністрування, а також органи державної влади, відповідальні за регулювання і контроль у сфері оподаткування. Особливу увагу приділено аналізу функціонування юридичних осіб, які формують та подають податкову звітність, використовуючи податкову інформацію у своїй діяльності. Такий підхід дозволив дослідити реальні механізми забезпечення конфіденційності податкової інформації та практичні виклики в її захисті.

Науково-практична значимість одержаних результатів полягає у формуванні рекомендацій щодо вдосконалення механізмів правового захисту податкової інформації, які можуть бути використані державними органами, що займаються адмініструванням податків, а також підприємствами для підвищення рівня інформаційної безпеки. Отримані результати можуть бути

впроваджені в освітній процес для підготовки фахівців у сфері оподаткування та правового забезпечення фінансової інформації.

Особистий внесок здобувача полягає у самостійному проведенні аналізу наукової літератури, нормативно-правових актів, а також вітчизняної та міжнародної практики захисту податкової інформації. Здобувачем розроблено пропозиції щодо покращення законодавчого регулювання і організаційних заходів із запобігання порушенням у сфері інформаційної безпеки, які представлені у кваліфікаційній роботі.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ ПРАВОВИХ АСПЕКТІВ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ

1.1 Поняття податкової інформації та правові засади конфіденційності, безпека податкової інформації.

Історичний розвиток поняття податкової інформації в юридичній науці та законодавстві має свої етапи, які можна розглянути за ключовими періодами.

Ранні етапи формування податкової інформації як поняття. На початкових стадіях розвитку державності й оподаткування інформація про платників податків і надходження не мала чіткого регламенту та переважно сприймалася як інструмент для управління ресурсами держави. У цей час відомості про платників часто збиралися місцевими правителями для контролю над економічною діяльністю і були обмеженими через відсутність організованих державних податкових структур.

Середньовіччя та початок систематизації податкової інформації. У період феодальних держав відбувається певна структуризація фінансових відомостей, що стосуються податків. Відомості про платників податків велися в різних формах реєстрів і були пов'язані з володінням майном або зобов'язанням сплачувати певні податки залежно від соціального статусу. Однак податкова інформація залишалася розрізненою і використовувалася переважно для підтримки місцевого адміністрування.

Розвиток капіталістичних відносин і систематизація податкової інформації. З розвитком капіталізму та зростанням потреб у державному фінансуванні в новітній час податкова інформація стає необхідним інструментом для забезпечення справедливого оподаткування. Законодавство деяких країн, зокрема Англії та Франції, починає передбачати збирання й облік інформації про доходи та майно. У цей період з'являються перші нормативні акти, які частково регулюють доступ до цієї інформації.

Сучасний етап розвитку податкового законодавства. Починаючи з ХХ століття, відбувається стандартизація процесів обробки та захисту податкової інформації на національному й міжнародному рівнях. Зокрема, законодавчі ініціативи передбачають обов'язковість звітування, реєстрації фінансових операцій, а також захист конфіденційності податкових даних. Суттєво вплинув розвиток цифрових технологій, що дозволило покращити обробку і захист інформації, а також спростити її передачу.

Розвиток міжнародних норм і рекомендацій. Зростання глобалізації призвело до розробки міжнародних стандартів щодо збирання, обробки та обміну податковою інформацією. Наприклад, Організація економічного співробітництва та розвитку (ОЕСР) розробила Рекомендації для запобігання ухиленню від оподаткування, що сприяло уніфікації вимог до податкової інформації на міжнародному рівні. Водночас значна увага приділяється конфіденційності та захисту таких даних.

Податкова інформація є складною юридичною категорією, яка включає в себе не лише дані про фінансові зобов'язання платників податків, але й відомості, що характеризують економічну діяльність суб'єктів господарювання, їхні фінансові результати та податкову звітність [1, с. 256].

Податкова інформація є важливим елементом правової системи, і вона поділяється на кілька видів, що мають значення в контексті податкового адміністрування. Одним із основних критеріїв для її класифікації є тип інформації. До такої інформації можна віднести, зокрема, дані про доходи та витрати платників податків. Ці відомості містять інформацію про те, які доходи отримує платник податків, а також які витрати пов'язані з його господарською діяльністю. Важливими також є дані про майно платника, що підлягає оподаткуванню. Це можуть бути відомості про нерухомість, транспортні засоби або інші активи, які підлягають оподаткуванню відповідно до законодавства. Крім того, велике значення має інформація про податкові зобов'язання платника, яка визначає суму податків і зборів, що повинні бути сплачені до бюджету. Не менш важливою є інформація, що

стосується виконання податкових зобов'язань. Це відомості, які підтверджують факт сплати податків, подачі податкових декларацій або інших звітних документів.

Крім того, податкову інформацію можна класифікувати за обсягом. Існує загальна інформація, яка стосується загального стану податкових зобов'язань, наприклад, загальної суми податкових надходжень або кількості платників податків. Вона має загальний характер і використовується для аналізу на макрорівні. Індивідуальна інформація, з іншого боку, містить конкретні дані про окремих платників податків, їхні доходи, податкові зобов'язання та сплату податків. Така інформація є важливою для конкретних перевірок або для використання в судових справах.

Ще одним критерієм класифікації податкової інформації є її джерело. Внутрішня податкова інформація — це ті дані, які збираються і обробляються податковими органами. Вона включає різноманітні документи, такі як податкові звіти, декларації, результати перевірок, а також інші відомості, що надаються платниками податків. Зовнішня податкова інформація включає дані, які надходять від третіх осіб або організацій, наприклад, від банків, контрагентів або інших державних органів. Ця інформація може бути використана для перевірки даних, наданих платниками податків, та для забезпечення належного контролю за виконанням податкових зобов'язань.

Таким чином, різноманітність видів податкової інформації відповідає різним правовим вимогам і є важливою для забезпечення ефективного податкового адміністрування.

Ці категорії дозволяють ефективно організувати податкову інформацію для її подальшого використання в адміністративному процесі, а також визначають правові аспекти доступу, використання та захисту цієї інформації.

Податкова інформація має кілька специфічних ознак, що відрізняють її від інших видів фінансової інформації, таких як бухгалтерська, корпоративна чи банківська.

Податкова інформація є частиною державного фінансового обліку і служить основним інструментом для визначення обсягу податкових зобов'язань платників податків. Вона зібрана і обробляється для виконання законодавчих вимог щодо сплати податків і зборів, в той час як інша фінансова інформація може бути спрямована на оцінку фінансового стану організацій, прийняття управлінських рішень або планування діяльності компаній. Наприклад, бухгалтерська інформація є внутрішнім інструментом для підприємств, а податкова — інструментом для взаємодії з державою.

Податкова інформація обов'язкова для надання і встановлюється відповідними законодавчими актами, що регулюють обов'язки платників податків. У той час як інша фінансова інформація може бути добровільною чи лише частково зобов'язуючою (наприклад, річний звіт компанії). Законодавчі вимоги щодо податкової інформації містять детальні інструкції щодо звітності, строків подачі, форм документів та санкцій за невиконання обов'язків.

Податкова інформація є особливо конфіденційною, оскільки вона містить персональні фінансові дані платників податків, що можуть впливати на їхні права та обов'язки. Законодавство визначає обмеження щодо доступу до податкової інформації для захисту прав платників. Для порівняння, інші види фінансової інформації, такі як загальні фінансові звіти компаній або банківські операції, можуть бути доступними більш широкому колу осіб за умов виконання відповідних вимог.

Захист податкової інформації має важливе значення для забезпечення стабільності економіки країни, адже недотримання конфіденційності може призвести до економічних втрат та порушення прав платників податків [2, с. 10-15].

Податкова інформація постійно змінюється в залежності від змін у податковому законодавстві, ставки податків, змін у фінансовому стані платників податків або виникнення нових видів податків. Крім того, податкова інформація повинна регулярно оновлюватися, зокрема, через

подання податкових декларацій або через зміни в податковому обліку. Це робить її більш динамічною порівняно з іншими видами фінансової інформації, які не завжди потребують такої частоти оновлення.

Податкова інформація є важливим елементом загальної інформаційної системи держави, і її функціонування має суттєве значення для організації економічного управління та фінансового контролю. Вона взаємодіє з іншими складовими державної інформаційної системи, зокрема з базами даних про соціальні виплати, митну інформацію, реєстраційні системи підприємств та особисті реєстри громадян. Це дозволяє створити комплексну мережу даних, що підтримують економічну безпеку держави і сприяють виконанню її політики.

Податкова інформація взаємодіє з іншими системами державного управління, наприклад, із системами соціального страхування, медичного обслуговування, земельного кадастру, реєстраційними системами власності тощо. Це дозволяє забезпечити цілісне бачення економічної діяльності платників податків і дає змогу державним органам ефективно оцінювати виконання не лише податкових, а й інших фінансових зобов'язань, зокрема в рамках соціальних і економічних програм.

Завдяки інтеграції податкової інформації в загальну інформаційну систему держави, забезпечується більша прозорість у взаємовідносинах між платниками податків і державними органами. Всі транзакції можна відслідковувати в реальному часі, що знижує ризики маніпуляцій і спрощує процедури податкового адміністрування. Зокрема, це стосується процесів обробки податкових декларацій і перевірок, що стало значно ефективнішим завдяки автоматизації.

Оскільки податкова інформація є конфіденційною і може впливати на права платників податків, її захист від несанкціонованого доступу є важливою складовою загальної інформаційної системи держави. Це включає не лише технічні аспекти, такі як криптографічний захист і багаторівневі

системи доступу, але й правові норми, що визначають порядок зберігання, обробки та передачі даних.

Податкова інформація, інтегрована в загальну інформаційну систему держави, сприяє оптимізації фінансового менеджменту, зниженню витрат на адміністрування, підвищенню ефективності контролю за виконанням податкових зобов'язань і зміцненню економічної стабільності держави.

Наукові підходи до класифікації податкової інформації варіюються в залежності від об'єкта дослідження (правові, технічні, організаційні аспекти).

Податкову інформацію можна класифікувати за її джерелами, такими як дані від платників податків (декларації, звіти), інформація, отримана від третіх осіб (наприклад, від банків чи митних органів), та офіційні документи, що містять державні норми і стандарти.

Правовий режим обробки податкової інформації зазвичай регламентується національним законодавством, яке визначає правила доступу до інформації, процедури її обробки і зберігання. Це включає в себе не тільки нормативні акти, але й міжнародні стандарти, що регулюють обробку фінансових даних, зокрема захист персональних даних і дотримання принципів конфіденційності та безпеки.

Правові рамки для захисту податкової інформації мають важливе значення для підтримки громадської довіри до податкових органів, і міжнародні угоди відіграють значну роль у гармонізації стандартів конфіденційності між країнами [3, р. 320].

Еволюція поняття податкової інформації у правовій доктрині має багатогранну історію, що відображає розвиток як законодавчої, так і наукової думки. Початково концепція податкової інформації була обмежена переважно обліковими та звітними функціями, однак з часом вона набула більш комплексного характеру, охоплюючи питання захисту даних, прав платників податків, а також адміністративної ефективності. Ключовими етапами цього розвитку стали зміни у податкових системах та адаптація

новітніх технологій, таких як автоматизація збору та обробки податкової інформації.

Практичне значення податкової інформації є надзвичайно важливим для адміністрування податків. Вона є основою для правильного обчислення податкових зобов'язань, виявлення порушень та здійснення заходів щодо запобігання ухиленню від сплати податків. Завдяки податковій інформації платники податків можуть реалізовувати свої права на справедливий розрахунок податків і доступ до публічної інформації, а податкові органи — ефективно контролювати дотримання законодавства.

Отже, поняття податкової інформації та правові засади її конфіденційності і безпеки є фундаментальними для забезпечення належного функціонування податкової системи та захисту прав платників податків. Правова регламентація цієї інформації охоплює широкий спектр аспектів, включаючи визначення її видів, обсягів, а також встановлення обмежень щодо доступу до неї. Забезпечення безпеки податкової інформації є важливим елементом для попередження можливих зловживань та порушень прав громадян. Відповідно, створення ефективної правової та технологічної інфраструктури для її захисту гарантує довіру до податкових органів та сприяє розвитку правової держави.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ ПРАВОВИХ АСПЕКТІВ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ

1.2. Законодавства щодо захисту податкової інформації національна та міжнародна практика.

Захист податкової інформації передбачає сукупність правових, організаційних, технічних і фізичних заходів, спрямованих на забезпечення конфіденційності, доступності та цілісності податкової інформації. Податкова інформація включає відомості, що стосуються фінансових зобов'язань платників податків, їх податкових декларацій, звітів, даних про майно, доходи та інші фінансові показники. Оскільки така інформація має важливе значення для держави та платників податків, її захист є важливою складовою частиною податкового адміністрування. Захист забезпечує недоторканність персональних даних платників податків, а також попереджає можливість їх неправомірного використання або розголошення.

Основні принципи захисту податкової інформації є конфіденційність, доступність, цілісність.

Конфіденційність є основним принципом захисту податкової інформації. Це означає, що доступ до податкової інформації обмежується лише тими особами або органами, яким надано відповідний дозвіл або права доступу. Цей принцип гарантує, що інформація не буде розголошена без належних підстав або у випадках, передбачених законодавством (наприклад, через рішення суду чи у рамках перевірок).

Доступність означає, що податкова інформація повинна бути доступною для органів влади та інших уповноважених суб'єктів для виконання їхніх функцій і обов'язків. Водночас, доступність не означає, що така інформація має бути загальнодоступною. Вона повинна бути доступною тільки у межах встановлених обмежень, для виконання законних обов'язків, таких як перевірки, податкові розрахунки або адміністративні заходи.

Цілісність інформації гарантує, що дані не будуть змінені, втрачені або пошкоджені в процесі зберігання, передачі чи обробки. Це забезпечується використанням спеціальних технічних засобів для захисту від несанкціонованого доступу або модифікацій, таких як шифрування, електронні підписи або інші засоби контролю за змінами в інформаційних системах.

Органи державної влади, зокрема податкові органи, несуть відповідальність за організацію та здійснення заходів для забезпечення захисту податкової інформації. Вони повинні дотримуватися встановлених норм і стандартів щодо збереження конфіденційності та безпеки даних, а також вчасно вживати заходів для запобігання витоку або несанкціонованого доступу до такої інформації. Порушення з боку органів влади можуть призвести до юридичних наслідків, включаючи штрафи або кримінальну відповідальність за неналежне виконання обов'язків щодо захисту даних.

Платники податків та інші суб'єкти, які мають доступ до податкової інформації, також несуть відповідальність за її захист. Це включає обов'язки щодо надання достовірних відомостей, а також забезпечення конфіденційності особистих та фінансових даних. У разі порушення вимог щодо захисту інформації платниками податків можуть бути застосовані штрафи або інші санкції відповідно до законодавства. Суб'єкти, які надають послуги з обробки або зберігання податкової інформації (наприклад, бухгалтери чи фінансові консультанти), також повинні дотримуватися стандартів безпеки та конфіденційності, оскільки порушення цих вимог може призвести до відповідальності як для них, так і для їхніх клієнтів.

Загалом, ефективний захист податкової інформації є критично важливим для забезпечення справедливості податкових відносин, захисту прав платників податків, а також для підтримання загальної стабільності фінансової системи держави.

Захист податкової інформації в Україні регулюється низкою законодавчих актів.

Податковий кодекс України, встановлює основні принципи адміністрування податків і зборів, а також захисту податкової інформації. Кодекс містить норми щодо конфіденційності даних, обмежень доступу до податкової інформації та відповідальності за порушення.

Закон України "Про захист персональних даних" цей закон визначає правові засади захисту персональних даних, у тому числі податкової інформації, що стосується фізичних осіб. Важливим аспектом є вимоги до обробки, зберігання, використання та передачі таких даних.

Закон України "Про інформацію" окреслює загальні положення, які регулюють доступ до публічної інформації, включаючи податкову, а також умови її захисту та обмеження доступу до неї.

Національне законодавство України у сфері захисту інформації включає норми Конституції, Закону України 'Про інформацію', а також спеціальних законів, які регулюють обробку податкових даних [4, с. 304].

Закон України "Про електронні документи та електронний документообіг" встановлює правила обробки електронних документів, що містять податкову інформацію, і забезпечує правову основу для використання електронних підписів і шифрування для забезпечення безпеки даних.

Кримінальний кодекс України містить статті, що передбачають кримінальну відповідальність за порушення законодавства щодо захисту інформації, зокрема за її незаконне використання або розголошення.

Практичні аспекти застосування національних норм щодо захисту податкової інформації.

Державна політика у сфері захисту інформації в інформаційно-комунікаційних системах спрямована на забезпечення конфіденційності, цілісності та доступності інформації, включаючи податкові дані [5].

На практиці застосування законодавства щодо захисту податкової інформації в Україні передбачає.

Використання технологій захисту інформації, застосування сучасних інформаційних технологій для шифрування та захисту податкових даних. Включає впровадження систем електронних декларацій і звітності, а також забезпечення їх захищеності від несанкціонованого доступу.

Інспекції та перевірки, податкові органи проводять перевірки для виявлення можливих порушень у сфері захисту податкової інформації, що включають випадки зловживань, крадіжки чи незаконного розповсюдження даних.

Обмеження доступу до даних, інформація про платників податків є конфіденційною, і доступ до неї має лише обмежене коло осіб: податкові органи, судові органи, уповноважені організації.

Обробка персональних даних у податковій сфері має здійснюватися з урахуванням принципу законності, конфіденційності та обмеження мети обробки, що прямо закріплено у національному законодавстві [6].

Навчання і сертифікація працівників, для забезпечення належного захисту інформації, працівники органів податкової служби, бухгалтерії та організацій, що займаються податковими питаннями, проходять відповідне навчання та сертифікацію з безпеки даних.

Для запобігання несанкціонованому доступу, втратам або маніпуляціям з податковими даними організації повинні відповідати міжнародним стандартам безпеки інформації, таким як ISO/IEC 27001 (система управління безпекою інформації). Це включає як фізичний, так і технічний захист даних, а також регулярний аудит систем.

Порядок визначає загальні вимоги до захисту податкової інформації, оброблюваної в інформаційно-комунікаційних системах, та встановлює правила доступу до таких даних [7, с.798-802].

Важливим аспектом є підготовка співробітників до роботи з конфіденційною податковою інформацією. Вони повинні знати не тільки законодавчі вимоги, а й практичні аспекти забезпечення безпеки інформації,

зокрема, уникати ситуацій, що можуть призвести до витоку або неналежного використання даних.

Загалом, національна практика захисту податкової інформації в Україні базується на законодавчих актах, що забезпечують високий рівень безпеки даних, ефективному контролю за їх зберіганням та обробкою, а також взаємодії різних органів для запобігання правопорушенням у цій сфері.

Отже, законодавство щодо захисту податкової інформації національне та міжнародне є важливою основою для забезпечення належного рівня безпеки та конфіденційності в податковій сфері. На національному рівні законодавчі акти, такі як закони про захист персональних даних та інформації в податкових органах, створюють чіткі механізми для контролю доступу та обробки податкової інформації. Міжнародні практики, зокрема стандартні механізми, розроблені Європейським Союзом і іншими міжнародними організаціями, надають додаткові інструменти для забезпечення захисту податкової інформації в умовах глобалізації. Ці правові норми, що інтегруються в національну правову систему, сприяють стандартизації процесів захисту, забезпечуючи гармонізацію національних та міжнародних вимог.

РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ПОДАТКОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ ПРАКТИЧНИЙ АНАЛІЗ СУЧАСНИХ ПРОБЛЕМ ТА ВИКЛИКІВ У ЗАХИСТІ ПОДАТКОВОЇ ІНФОРМАЦІЇ

2.1. Види правового режиму податкової інформації.

Правовий режим податкової інформації визначає порядок збору, обробки, зберігання, передачі та захисту інформації, пов'язаної з податковими відносинами. Він базується на нормах права, що регулюють доступ до інформації, її конфіденційність, використання та обмеження. Види правового режиму податкової інформації можна класифікувати за кількома критеріями.

Податкову інформацію можна класифікувати й за рівнем доступу до неї, що важливо для визначення, хто може отримувати певні дані, а також у яких умовах ці дані можуть бути використані. Загальнодоступна податкова інформація є відомостями, які можуть бути вільно доступні для широкого кола осіб. Це може бути інформація про загальний стан податкових надходжень, кількість платників податків, або інші статистичні дані, які не містять приватних відомостей і не потребують особливого захисту. Обмежено доступна податкова інформація включає дані, доступ до яких обмежений певним колом осіб або організацій, зокрема спеціально уповноваженими посадовими особами або установами, що мають відповідні повноваження. Така інформація може включати відомості, які є важливими для виконання обов'язків податковими органами, але не підлягають загальному доступу. Конфіденційна податкова інформація, в свою чергу, стосується даних, доступ до яких строго обмежений і зазвичай доступний лише для самого платника податків та відповідних державних органів. Це можуть бути відомості про особисті доходи, майно, податкові зобов'язання та інші дані, що містять приватну інформацію, яку необхідно захищати законом.

Що стосується характеру використання податкової інформації, то можна виділити два основних напрямки. Інформація, що використовується для податкових цілей, є основною для діяльності податкових органів і використовується безпосередньо для визначення та виконання податкових зобов'язань платників податків. Вона може включати дані про доходи, витрати, майно, а також звіти і декларації платників податків. Інформація, що використовується для адміністративних і правоохоронних цілей, охоплює відомості, які можуть бути використані іншими державними органами, такими як правоохоронні органи, для проведення перевірок, розслідувань або для забезпечення правопорядку в контексті виконання податкових зобов'язань.

Нарешті, податкову інформацію можна класифікувати за суб'єктами обробки. Інформація, що обробляється податковими органами, стосується відомостей, які збираються і обробляються безпосередньо органами, відповідальними за податкову політику і адміністрування податків. Це основний потік даних, необхідних для контролю за дотриманням податкових зобов'язань. Інформація, що обробляється іншими державними органами, включає дані, які можуть бути отримані або використовувані іншими органами державної влади, наприклад, правоохоронними органами або органами статистики, для виконання своїх функцій і забезпечення правопорядку.

Таким чином, класифікація податкової інформації за рівнем доступу, характером використання та суб'єктами обробки є важливим аспектом, що забезпечує ефективну організацію податкового контролю та захисту прав платників податків.

Рівень доступу до податкової інформації визначає її правовий режим, що встановлює межі використання, захисту та розкриття даних. Податкова інформація може бути загальнодоступною, обмежено доступною або конфіденційною, залежно від її змісту, важливості та потенційного впливу на

права платників податків і державні інтереси. Такий підхід забезпечує баланс між прозорістю податкової системи та захистом чутливих даних.

Податкова інформація може бути класифікована за правовим режимом на публічну, з обмеженим доступом і внутрішньослужбову інформацію залежно від суб'єкта доступу [8, с.320].

Загальнодоступна податкова інформація — це відомості, що можуть бути вільно використані будь-якими зацікавленими особами без необхідності отримання спеціального дозволу. Її основною метою є забезпечення прозорості податкової системи, формування довіри громадськості до податкової політики, а також підвищення рівня обізнаності платників податків про їхні права та обов'язки.

До цієї категорії належать статистичні дані щодо податкових надходжень до бюджету, актуальні податкові ставки, умови застосування податкових пільг, а також нормативно-правові акти, що регулюють податкові відносини. Наприклад, це можуть бути відомості про ставки податку на доходи фізичних осіб, податку на додану вартість, акцизи або митні збори. Усі ці дані є важливими для забезпечення правової визначеності та однакового застосування норм податкового законодавства.

Правовий режим загальнодоступної податкової інформації передбачає її розміщення у відкритих джерелах, таких як офіційні вебсайти податкових органів, інформаційні бюлетені або державні реєстри. Інформація повинна бути актуальною, достовірною та доступною для ознайомлення без додаткових перешкод. Відповідальність за це покладається на державні органи, зокрема на Державну податкову службу України. Законодавство України, зокрема Закон "Про доступ до публічної інформації" та Податковий кодекс України, зобов'язують відповідні органи оприлюднювати подібні дані з метою інформування громадян.

Важливо, що загальнодоступна інформація не потребує ідентифікації осіб, які бажають нею скористатися, та не передбачає юридичних чи технічних бар'єрів для її поширення. Це гарантує легкий доступ до

необхідних даних, забезпечує прозорість дій податкових органів та сприяє формуванню довіри громадськості до державної податкової політики.

Таким чином, загальнодоступна податкова інформація є ключовим елементом демократичного управління та ефективного функціонування податкової системи, забезпечуючи реалізацію принципів прозорості, підзвітності та правової визначеності.

Правовий режим податкової інформації забезпечується на основі принципів законності, прозорості та конфіденційності. Основними режимами є публічний і конфіденційний доступ [9, с. 256].

Обмежено доступна податкова інформація охоплює дані, доступ до яких надається лише певним особам або організаціям за наявності законних підстав. Така інформація є частиною податкової системи, але її поширення обмежується для забезпечення конфіденційності та захисту інтересів платників податків і держави.

До обмежено доступної інформації належить, наприклад, зведена фінансова інформація про діяльність підприємств або окремих платників податків, яка використовується для податкового контролю чи аналітики. Відомості такого характеру не підлягають публічному розголошенню і можуть бути надані лише за спеціальними запитами з боку уповноважених органів, наприклад, правоохоронних або контролюючих організацій.

Правовий режим цієї категорії інформації визначається необхідністю її захисту від неправомірного розголошення чи використання.

Доступ до інформації, регламентується спеціальними нормами законодавства, такими як Податковий кодекс України та Закон України "Про захист персональних даних".

Передача даних, можлива лише за умови дотримання встановлених процедур, наприклад, за запитом суду, слідчих органів або в межах податкової перевірки.

Захист інформації, передбачає відповідальність за її незаконне поширення, у тому числі адміністративну та кримінальну відповідальність відповідно до чинного законодавства.

Крім того, особливий акцент робиться на впровадженні сучасних технічних заходів безпеки для запобігання несанкціонованому доступу до інформації. Це включає шифрування даних, багаторівневий контроль доступу та регулярний моніторинг систем безпеки.

Таким чином, обмежено доступна податкова інформація виконує важливу роль у забезпеченні функціонування податкової системи, залишаючись доступною лише в межах, необхідних для законного використання. Такий підхід сприяє збереженню балансу між прозорістю та захистом прав платників податків.

Інформація, що обробляється в податкових органах, може бути віднесена до різних видів правового режиму: відкритої, конфіденційної чи інформації з обмеженим доступом [10].

Характер використання податкової інформації визначає її функціональне призначення в системі державного управління та контролю. Інформація може застосовуватись виключно для податкових цілей або в межах адміністративних і правоохоронних процедур. Такий поділ забезпечує ефективність обробки даних та дотримання законності їх використання.

Інформація, що використовується для податкових цілей, охоплює дані, необхідні для забезпечення належного функціонування податкової системи. Вона включає податкові декларації, розрахунки податкових пільг, відомості про доходи, витрати та фінансовий стан платників податків. Головне призначення таких даних — нарахування податкових зобов'язань, проведення перевірок, контролю за виконанням податкових обов'язків і адміністрування податків.

Правовий режим, інформація цієї категорії має обмежений доступ і може використовуватися виключно податковими органами для виконання їхніх функцій. Використання таких даних поза межами податкового

адміністрування суворо заборонено та підлягає юридичній відповідальності. Законодавство передбачає чіткі правила захисту таких даних, зокрема щодо конфіденційності та цільового використання, щоб запобігти їхньому неправомірному розголошенню чи використанню.

Інформація, що використовується для адміністративних і правоохоронних цілей, має більш широкий спектр застосування порівняно з даними, призначеними виключно для податкових цілей. Вона залучається у випадках, пов'язаних із судовими процесами, розслідуваннями фінансових злочинів, перевітками дотримання законодавства, включно з податковими, але не обмежуючись ними. Наприклад, такі дані можуть включати інформацію про ухилення від сплати податків, відомості про фінансові операції, що викликають підозру, або сліди незаконного збагачення.

Правовий режим, ця категорія інформації перебуває під особливим контролем для забезпечення законності її використання. Податкові органи, правоохоронні органи, суди та інші компетентні структури мають право доступу до таких даних лише за умови дотримання встановлених процедур, зокрема за наявності відповідного запиту, ухвали суду чи іншого юридичного дозволу. Використання цієї інформації поза межами визначених законом цілей або розголошення без належної підстави може спричинити серйозні правові наслідки.

Податкова інформація класифікується за режимами доступу: публічна, обмежена в доступі (конфіденційна), службова та секретна інформація залежно від змісту і значущості для держави [11].

За суб'єктами обробки податкової інформації можна розрізняти дані, що обробляються різними органами відповідно до їхніх повноважень. Це можуть бути як податкові органи, які здійснюють основну роботу з адміністрування податків, так і інші державні структури, наприклад, правоохоронні органи, які використовують податкову інформацію в рамках розслідувань або виконання правозастосовних функцій. Різний статус суб'єктів обробки визначає правила доступу до даних та умови їхнього використання.

Інформація, що обробляється податковими органами, охоплює всі дані, які збираються та використовуються податковими службами для виконання їхніх основних функцій, таких як адміністрування податків, контроль за сплатою податків та проведення податкових перевірок. Це може включати податкові декларації платників податків, звіти про доходи та витрати, документи про перевірки та інші матеріали, що стосуються виконання податкових зобов'язань.

Режим доступу до податкової інформації залежить від рівня захисту даних і розподіляється на загальнодоступний та захищений відповідно до законодавства України [12].

Правовий режим, обробка такої інформації регулюється низкою законів, зокрема законами, що визначають функції податкових органів, а також нормативно-правовими актами, що забезпечують захист інформації. Податкові органи зобов'язані дотримуватися законодавчих вимог щодо конфіденційності, цілісності та доступності цих даних. Крім того, за порушення умов обробки такої інформації можуть бути застосовані санкції, включаючи відповідальність за неправомірне використання або розголошення даних.

Податкова інформація в залежності від її змісту та правового режиму може бути поділена на відкриту, конфіденційну та службову. Ці режими регламентують правила її зберігання та розкриття [13, с.380].

Отже, види правового режиму податкової інформації визначаються різноманітністю підходів до класифікації та обробки даних в контексті правових норм та стандартів. Враховуючи важливість податкової інформації для забезпечення фінансової стабільності, різні правові режими дозволяють ефективно контролювати доступ до таких даних, забезпечуючи їх належний захист. Протягом аналізу виділені категорії, такі як конфіденційна, обмежено доступна та загальнодоступна інформація, кожна з яких має свою специфіку обробки та використання. Законодавчі механізми та нормативні акти, що регулюють ці режими, створюють основи для безпечного та ефективного

функціонування податкової системи, водночас гарантуючи захист прав платників податків та інших учасників податкових відносин.

РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ПОДАТКОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ ПРАКТИЧНИЙ АНАЛІЗ СУЧАСНИХ ПРОБЛЕМ ТА ВИКЛИКІВ У ЗАХИСТІ ПОДАТКОВОЇ ІНФОРМАЦІЇ

2.2. Випадки порушення захисту податкової інформації.

Причини порушень захисту податкової інформації можуть бути різноманітними, серед яких найпоширенішими є людський фактор, технічні недоліки та прогалини в законодавчому забезпеченні. Людський фактор включає недбалість або свідоме порушення з боку працівників, що обробляють інформацію, а також зловмисний доступ до даних. Технічні проблеми виникають через уразливості в інформаційних системах, що не забезпечують належний рівень захисту від кіберзагроз. Проблеми законодавства, зокрема неузгодженість та застарілість норм, можуть ускладнити ефективний захист податкової інформації, що дозволяє порушникам маніпулювати даними без належних правових наслідків.

Людський фактор є однією з найбільш значущих причин порушень захисту податкової інформації. В першу чергу, це стосується невірнього або недбалого поводження з інформацією працівниками, які мають доступ до чутливих даних. Наприклад, недотримання правил безпеки при обробці або зберіганні податкових документів, а також несанкціоноване поширення або використання інформації через помилки в процесі роботи. Така недбалість може призвести до витоку конфіденційних відомостей, що суттєво підриває довіру до системи податкової безпеки.

Основними порушеннями захисту податкової інформації виявлено витоки даних під час передачі їх між інформаційними системами, що виникають через недотримання правил шифрування [14].

Наступною причиною є можливість несанкціонованого доступу через внутрішні помилки або безвідповідальність працівників. У деяких випадках, організаційні недоліки, як-от неналежний контроль за доступом до

податкової інформації або відсутність чітко визначених процедур для перевірки доступу, можуть призвести до того, що особи без необхідних повноважень зможуть потрапити до чутливої інформації. Безвідповідальність у впровадженні політики доступу або недотримання встановлених процедур можуть стати основними факторами, які знижують рівень безпеки даних.

Порушення порядку доступу до персональних даних, які містяться в податковій інформації, є підставою для адміністративної та кримінальної відповідальності [15].

Одним із поширених випадків порушення є несанкціонований доступ працівників податкових органів до інформації, що не пов'язана з їх посадовими обов'язками [16, с. 157].

Не менш важливою причиною є несанкціоноване поширення або розголошення інформації через зловмисні наміри. В деяких випадках працівники можуть свідомо порушувати закон, передаючи або публікуючи конфіденційну податкову інформацію з особистих чи інших мотивів. Це може статися через корупційні схеми або спроби отримати матеріальну вигоду за рахунок розголошення важливих даних. Така поведінка не лише порушує законодавство, а й підриває довіру до податкової системи та її здатність захищати права платників податків.

Технічні недоліки та кіберзагрози становлять серйозну загрозу для захисту податкової інформації, оскільки сучасні інформаційні системи, які використовуються для зберігання та обробки податкових даних, можуть мати уразливості, що дають змогу зловмисникам отримувати доступ до чутливої інформації. Однією з основних причин порушень є відсутність належного шифрування даних, що забезпечує конфіденційність і захист інформації. Без ефективних методів шифрування дані можуть бути легко перехоплені під час передачі або в разі несанкціонованого доступу до баз даних.

Ще однією серйозною проблемою є атаки хакерів, що використовують різноманітні методи, щоб обійти захисні механізми інформаційних систем. Хакери можуть виявити вразливості в програмному забезпеченні або

зловживати недосконалою системою контролю доступу, щоб отримати доступ до конфіденційних податкових даних. Такі атаки можуть мати значні наслідки, включаючи виток персональних даних платників податків або викрадення важливої фінансової інформації, що порушує законодавство та може призвести до великих фінансових втрат.

У 2022 році було зафіксовано понад 50 випадків витоку податкової інформації через фішингові атаки, спрямовані на працівників податкових органів [17, с. 9].

Не менш важливими є технічні помилки або збої в системах безпеки, які можуть статися внаслідок неправильно налаштованих систем або програмного забезпечення. Наприклад, помилки в налаштуванні параметрів безпеки можуть дозволити несанкціонованим особам отримати доступ до конфіденційних даних або порушити цілісність інформації. Крім того, збій у системах безпеки може призвести до тимчасової втрати або пошкодження даних, що також може мати серйозні наслідки для надійності податкової системи та забезпечення прав платників податків.

Більшість порушень у сфері податкової інформації стосується використання застарілих засобів захисту даних, що робить їх вразливими до кібератак [18, с. 312].

Проблеми в законодавчому та нормативному забезпеченні захисту податкової інформації стають однією з основних причин порушень безпеки даних. Недосконалість нормативно-правових актів, що регулюють захист податкової інформації, створює правову невизначеність, яка може бути використана для обходу стандартів безпеки. Законодавство не завжди встигає швидко реагувати на нові технологічні виклики, що виникають у сфері захисту даних, що може спричинити низку юридичних прогалин.

Однією з найбільших проблем є неузгодженість та застарілість законодавства, що пов'язано з постійно змінюваними умовами технологічного розвитку. Наприклад, застарілі норми захисту персональних даних не можуть ефективно справлятися з новими загрозами, які виникають

внаслідок інтернет-атака чи зловживання інформаційними системами. Законодавчі прогалини, зокрема відсутність актуальних норм для захисту податкової інформації у умовах масового використання цифрових технологій, значно ускладнюють забезпечення ефективної безпеки даних.

Одним із наймасштабніших порушень стало зловживання службовими обов'язками співробітниками державних установ, які передавали податкові дані третім особам за винагороду [19].

Також існують прогалини в правових актах, що не дозволяють належним чином регулювати нові аспекти захисту податкової інформації, які виникають через розвиток технологій. Наприклад, не всі законодавчі акти враховують новітні способи обробки даних, такі як використання хмарних технологій чи великих даних (big data), що може створювати додаткові ризики для безпеки інформації. У результаті, правовий захист податкової інформації виявляється недостатнім у нових технологічних умовах.

Несанкціонований доступ до податкової інформації є одним із ключових ризиків для захисту даних. Часто це трапляється через отримання доступу до податкової інформації без належних повноважень, що може бути результатом як умисних дій, так і недоліків у системах контролю доступу.

Також значну загрозу становлять зломи або порушення безпеки інформаційних систем органів податкової служби, які зазвичай здійснюються хакерами чи іншими зловмисниками з метою отримання чутливої інформації для використання в шахрайських схемах або продажу.

Окрему небезпеку становить порушення конфіденційності співробітниками органів податкової служби, які можуть навмисно або через недбалість передати інформацію третім особам. Такі випадки зазвичай свідчать про відсутність належного моніторингу та запобіжних заходів з боку керівництва.

Розголошення або публікація конфіденційної інформації є серйозним порушенням, яке може призводити до значних наслідків як для платників податків, так і для державної системи.

Одним із найпоширеніших прикладів є неправомірне розкриття персональних даних платників податків, що порушує принципи конфіденційності. Це може включати оприлюднення інформації про доходи, податкові декларації чи інші персональні відомості.

Фіксуються випадки неправомірного доступу до податкової інформації через недосконалість процесів автентифікації у внутрішніх системах [20].

Також небезпечним є публікація чи передача податкової інформації, що порушує права та свободи громадян. Це може відбуватися як через навмисні дії осіб, що мають доступ до даних, так і через недоліки у захисті інформаційних систем.

Окремо виділяється розголошення даних підприємств, які містять комерційну таємницю або інші захищені законом відомості. Такі дії можуть завдати шкоди репутації бізнесу, спричинити фінансові втрати та створити конкурентні переваги для третіх осіб.

Зловживання податковою інформацією органами влади або іншими особами становить одну з найсерйозніших загроз для довіри громадян до державної системи.

По-перше, це може включати використання податкової інформації для політичних або економічних цілей, наприклад, для тиску на опонентів, просування інтересів окремих груп чи осіб, або створення несправедливих умов для бізнесу.

Другою важливою проблемою є вилучення або збереження податкової інформації для неправомірних дій або особистої вигоди. Така практика може включати передачу даних третім сторонам, використання інформації для отримання хабарів або інших незаконних вигод.

Третій аспект — це надмірне або непотрібне розкриття інформації без належних юридичних підстав, яке часто маскується під офіційні запити чи адміністративні процедури. Це порушує принципи законності та пропорційності в обробці податкових даних.

Такі зловживання підривають принципи прозорості та законності, створюючи ризики для ефективного функціонування податкової системи.

Отже, випадки порушення захисту податкової інформації є серйозною загрозою для стабільності та довіри до податкової системи. Аналіз таких інцидентів показує, що вони можуть виникати через різноманітні фактори, зокрема недостатній рівень захисту інформаційних систем, людський фактор, а також несанкціонований доступ з боку третіх осіб. Важливо, щоб податкові органи впроваджували ефективні заходи для виявлення та усунення вразливих місць, а також здійснювали моніторинг та аудит систем безпеки. Навчання співробітників, удосконалення технологічних засобів захисту та зміцнення правових механізмів дозволяють знижувати ризики порушення захисту податкової інформації та покращувати загальну інформаційну безпеку.

РОЗДІЛ 2. ПРАВОВИЙ РЕЖИМ ПОДАТКОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ ПРАКТИЧНИЙ АНАЛІЗ СУЧАСНИХ ПРОБЛЕМ ТА ВИКЛИКІВ У ЗАХИСТІ ПОДАТКОВОЇ ІНФОРМАЦІЇ

2.3. Способи попередження порушень та зловживань у сфері захисту податкової інформації.

Зміцнення законодавчої та нормативної бази є ключовим елементом у попередженні порушень захисту податкової інформації. Перш за все, необхідно розробити та вдосконалити законодавчі акти, які регулюють захист податкової інформації на рівні як національного, так і міжнародного законодавства. Це передбачає не тільки уточнення існуючих норм, але й створення нових нормативних актів, що враховують сучасні технологічні досягнення та новітні загрози в інформаційній сфері. Наприклад, слід впровадити чіткі визначення щодо типів інформації, що підлягає захисту, а також розмежувати права доступу до цієї інформації залежно від її рівня конфіденційності.

Важливим аспектом є уніфікація стандартів захисту даних на національному та міжнародному рівнях. Глобалізація інформаційних технологій та зростання міжнародних економічних і політичних зв'язків вимагають узгодження стандартів захисту даних, що дозволить ефективно обмінюватися податковою інформацією між державами, зберігаючи при цьому належний рівень конфіденційності. У цьому контексті важливо враховувати міжнародні угоди та ініціативи, такі як Регламент Європейського Союзу щодо захисту персональних даних (GDPR) або стандарти, розроблені Організацією економічного співробітництва та розвитку (ОЕСР), які регламентують обмін податковою інформацією між країнами.

Також слід створити чіткі правові механізми для боротьби з порушеннями в сфері захисту податкової інформації. Це включає не лише

розробку механізмів відповідальності за порушення норм захисту інформації, але й визначення заходів щодо забезпечення виконання законодавчих вимог. Це може включати встановлення санкцій за несанкціонований доступ до податкової інформації, а також за розголошення або неналежне використання такої інформації. Важливо, щоб такі заходи були ефективними та забезпечували належний рівень захисту прав платників податків та державних інтересів.

Впровадження сучасних систем шифрування та захисту даних є одним з основних елементів забезпечення безпеки податкової інформації. У сучасних умовах, коли інформація передається і зберігається в електронному вигляді, захист даних за допомогою шифрування стає необхідністю. Шифрування дозволяє перетворювати дані на незрозумілу послідовність символів, яку можна повернути до початкового вигляду лише за допомогою спеціального ключа. Це забезпечує високий рівень конфіденційності, навіть якщо дані потрапляють до несанкціонованих осіб. Для податкових органів важливо не лише використовувати стандартні методи шифрування, а й застосовувати сучасні, більш складні системи, які здатні забезпечити максимальний рівень захисту даних у випадку, якщо зловмисники намагаються порушити цілісність інформації.

Одним з найперспективніших напрямів у забезпеченні безпеки інформації є використання біометричних та інших високотехнологічних засобів для контролю доступу. Біометрія, зокрема, використання відбитків пальців, розпізнавання обличчя або райдужної оболонки ока, дозволяє точно ідентифікувати особу, що намагається отримати доступ до захищених систем. Це значно знижує ризики несанкціонованого доступу, оскільки біометричні характеристики є унікальними для кожної людини і їх неможливо підробити чи забути, як це може статися з паролями чи іншими традиційними методами автентифікації. Крім того, в умовах, коли обробка податкової інформації здійснюється на кількох рівнях (платники податків, податкові органи, аудитори тощо), використання біометричних систем забезпечує надійний

контроль доступу до чутливої інформації, що в свою чергу мінімізує можливість зловживань або витоків даних.

Ефективне попередження зловживань у сфері податкової інформації базується на застосуванні багатофакторної автентифікації та регулярному проведенні аудиту інформаційних систем [21, с. 312].

Не менш важливим елементом у забезпеченні захисту податкової інформації є регулярні аудити безпеки інформаційних систем. Аудити безпеки спрямовані на виявлення уразливих місць у системах захисту, що можуть бути використані зловмисниками для несанкціонованого доступу або зміни даних. Регулярний аудит дозволяє своєчасно виявляти проблеми, що можуть виникнути в процесі обробки та зберігання інформації, і вжити заходів для їх усунення. Це не лише допомагає підтримувати високий рівень безпеки, але й дає змогу організаціям, що займаються податковим адмініструванням, оперативно реагувати на нові загрози, які з'являються у результаті розвитку технологій або зміни кіберзлочинних методів. Аудит безпеки також включає перевірку на відповідність нормативним вимогам, що дозволяє визначити, чи відповідає система захисту податкової інформації вимогам законодавства та міжнародних стандартів.

Серед ключових способів попередження порушень виділяють навчання персоналу основам кібербезпеки та впровадження протоколів реагування на інциденти [22, с. 284].

Важливою складовою частиною процесу забезпечення захисту податкової інформації є навчання та підвищення кваліфікації персоналу. З огляду на те, що людський фактор є однією з основних причин порушень безпеки інформації, необхідно здійснювати постійне навчання працівників, які мають доступ до податкової інформації, щодо правил безпеки і кращих практик захисту даних. Це включає навчання правильному поведінню з інформацією, обробці даних згідно з політиками конфіденційності, а також реагуванню на інциденти, що можуть виникнути в процесі роботи з чутливою інформацією. Крім того, необхідно регулярно оновлювати знання

співробітників у сфері кібербезпеки, оскільки технології постійно змінюються і з'являються нові загрози. Організація тренінгів з кіберзахисту, забезпечення знань про основні види загроз (фішинг, віруси, атаки на інформаційні системи) допомагає мінімізувати ризики від помилок персоналу.

Для попередження несанкціонованого доступу до інформаційних систем рекомендується застосовувати сертифіковані засоби криптографічного захисту інформації [23].

Проведення тренінгів та навчань для працівників, які працюють з податковою інформацією, є ключовим елементом у забезпеченні належного рівня захисту даних. Враховуючи, що значна частина порушень безпеки інформації виникає через людський фактор, регулярне навчання персоналу допомагає зменшити ймовірність таких інцидентів. Працівники, які мають доступ до чутливої податкової інформації, повинні бути добре обізнані з основними принципами конфіденційності та безпеки. Вони повинні розуміти не тільки технологічні аспекти захисту даних, а й етичні норми, що регулюють роботу з податковою інформацією.

Впровадження політики безпеки та етики щодо роботи з конфіденційними даними є наступним важливим кроком у забезпеченні захисту податкової інформації. Політика безпеки повинна визначати чіткі правила доступу до податкової інформації, її обробки та зберігання. Вона повинна містити положення щодо обов'язків працівників при роботі з чутливими даними, включаючи заборону на несанкціоноване копіювання або передачу інформації, а також на використання особистих пристроїв для доступу до систем. Крім того, етичні стандарти повинні наголошувати на необхідності збереження конфіденційності та чесності в процесі роботи з податковими даними, що є важливим для підтримки довіри платників податків до системи.

Контроль та моніторинг дій органів влади та суб'єктів податкових правовідносин є важливим елементом у загальній системі захисту податкової інформації. Важливою складовою цього процесу є встановлення чітких

механізмів моніторингу діяльності, що дозволяють вчасно виявити порушення або зловживання під час обробки податкової інформації. Це може включати контроль за доступом до баз даних, реєстрацію всіх спроб доступу та редагування інформації, а також нагляд за відповідністю процедур обробки даних вимогам законодавства. Моніторинг має також включати перевірку дій службовців податкових органів та інших осіб, які працюють з податковою інформацією, на наявність можливих порушень або зловживань.

Регулярна актуалізація програмного забезпечення є ключовим інструментом для захисту податкової інформації від сучасних кіберзагроз [24, с. 112-114].

Стандарти передбачають впровадження політики мінімізації доступу, коли кожен співробітник має доступ лише до тієї інформації, яка необхідна для виконання посадових обов'язків [25, с. 45].

Ефективний внутрішній контроль передбачає створення багаторівневої системи нагляду, що включає автоматизовані та ручні методи перевірки. Автоматизовані системи можуть бути оснащені алгоритмами для моніторингу та аналізу великих обсягів інформації, що дозволяє оперативно виявляти порушення, зловживання або неналежне зберігання даних. Такі системи повинні бути інтегровані з іншими інформаційними системами державних органів, що дозволяє забезпечити швидкий доступ до необхідних даних та відстеження їхнього використання на всіх етапах обробки. Це включає відслідковування всіх змін в електронних базах даних, реєстрацію усіх дій щодо податкової інформації, а також фіксацію доступу до чутливих даних.

Загалом, розвиток механізмів внутрішнього контролю за обробкою та зберіганням податкової інформації, створення незалежних органів для моніторингу порушень, залучення аудиторів та перевірок, а також підвищення прозорості і довіри є важливими складовими для створення ефективної та безпечної системи обробки податкової інформації. Лише за умови належного контролю, постійного аудиту та взаємодії з громадськістю

можна забезпечити високий рівень безпеки, що є необхідним для стабільної роботи податкової системи та підтримки довіри до органів державної влади.

Невід'ємною частиною цих кампаній має бути надання чітких інструкцій для підприємств, які повинні дотримуватись особливих вимог щодо обробки податкової інформації. Вони мають знати, як забезпечити безпеку даних, яких заходів необхідно вживати для захисту від несанкціонованого доступу і як правильно поводитися з конфіденційними даними. Зокрема, роз'яснювальна робота повинна охоплювати теми використання захищених систем для передачі даних, правильного зберігання податкових звітів та інших документів, а також навчання підприємців щодо важливості регулювання доступу до цієї інформації в межах своїх організацій.

Європейські практики акцентують на впровадженні систем моніторингу активності користувачів та автоматизованого виявлення аномальної поведінки для запобігання інцидентам [26, с. 38].

Міжнародний досвід може стати важливим елементом для розробки нових підходів до захисту податкової інформації, враховуючи специфіку законодавства різних країн та регіонів. Також варто відзначити, що міжнародні стандарти, якщо вони будуть узгоджені на глобальному рівні, дозволять знизити рівень протиріч у національних правових системах і полегшити інтеграцію між різними юрисдикціями.

Загалом, ефективний захист податкової інформації вимагає комплексного підходу, який включає встановлення чітких стандартів обміну даними між державними органами, активну освітню кампанію серед громадян і підприємств, а також міжнародну співпрацю для вдосконалення загальних принципів захисту даних. Такий підхід забезпечить надійність і безпеку податкових систем, а також сприятиме розвитку взаємодії між різними державами в контексті глобальної економіки.

Серед найбільш ефективних способів попередження порушень – використання інтегрованих рішень на основі штучного інтелекту, які дозволяють ідентифікувати ризики у реальному часі [27, с. 16].

Отже, способи попередження порушень та зловживань у сфері захисту податкової інформації є критично важливими для забезпечення надійності та ефективності системи оподаткування. Застосування профілактичних заходів, таких як регулярні аудити, моніторинг доступу до даних, а також вдосконалення законодавчої бази і посилення відповідальності за порушення, дозволяють значно зменшити ймовірність зловживань та несанкціонованого доступу. Водночас, важливим аспектом є навчання та підвищення обізнаності працівників податкових органів про можливі загрози і кращі практики безпеки. Комплексний підхід до запобігання порушень сприяє не лише захисту податкової інформації, а й зміцненню довіри до системи оподаткування та забезпеченню її стабільності в умовах сучасних викликів.

РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ

3.1. Технологічні засоби захисту та організаційні заходи для запобігання не санкційованому доступу.

Технологічні засоби захисту податкової інформації є важливою складовою стратегії безпеки в умовах сучасних загроз, пов'язаних із цифровою трансформацією. Для забезпечення належного рівня захисту даних, що зберігаються і передаються, використовуються різноманітні технології та інструменти. Одним із ключових напрямків є впровадження сучасних систем шифрування та захисту даних. Ці системи дозволяють гарантувати безпеку інформації як під час її зберігання, так і при передачі через канали зв'язку. Використання алгоритмів шифрування, таких як AES і RSA, створює надійний захист, перетворюючи дані в незрозумілу форму без відповідного ключа, що унеможливорює доступ сторонніх осіб.

Системи багаторівневого захисту, включаючи шифрування даних і біометричну автентифікацію, забезпечують надійний бар'єр проти несанкціонованого доступу [28, с. 320].

Для захисту від шкідливих програм, які можуть бути використані для проникнення в інформаційні системи, впроваджуються антивірусні та антипоштові системи. Ці програми здійснюють постійний моніторинг мережових з'єднань і файлів, блокуючи потенційно небезпечний контент, що може призвести до витоку або пошкодження даних.

Побудова інформаційної безпеки базується на розробці політики мінімізації доступу, постійному оновленні систем безпеки та навчанні персоналу [29, с. 276].

З боку організаційних заходів основним є розробка та впровадження політик доступу та контролю. Це включає в себе чітке визначення, хто має право доступу до податкової інформації, в яких межах і з якою метою. Важливо, щоб доступ надавався лише тим особам, для яких ця інформація

необхідна для виконання своїх обов'язків, що мінімізує ймовірність її несанкціонованого використання.

Реалізація багатофакторної автентифікації та регулярні аудити систем є обов'язковими елементами сучасного захисту інформації [30, с. 24].

Не менш важливим є навчання та підвищення кваліфікації персоналу. Регулярні тренінги та семінари з питань безпеки допомагають працівникам краще розуміти важливість захисту інформації та правильно поводитися з конфіденційними даними. Це також включає інформування про останні загрози та нові методи захисту, що дозволяє оперативно адаптуватися до змінюваних умов.

Розробка внутрішніх інструкцій та протоколів є наступним важливим кроком у забезпеченні безпеки. Детальні інструкції з обробки та доступу до податкової інформації мають бути чіткими і відповідати актуальним вимогам законодавства та технологічним стандартам. Це дозволяє систематизувати процеси, уникнути помилок і забезпечити належний рівень контролю.

Загалом, забезпечення захисту податкової інформації є багатогранним процесом, що поєднує технологічні засоби, організаційні заходи і відповідальність усіх учасників процесу. Це дозволяє створити надійну систему захисту, що мінімізує ризики витоків і зловживань, забезпечуючи належний рівень конфіденційності та цілісності даних.

Використання систем реального часу для моніторингу кіберзагроз дозволяє знизити ризик несанкціонованого доступу [31, с. 298].

Системи шифрування та захисту даних є одними з найважливіших технологічних засобів для забезпечення безпеки податкової інформації. Вони використовуються для захисту даних як під час їх зберігання, так і при передачі через різні канали комунікацій, що робить їх незамінним інструментом у боротьбі з несанкціонованим доступом до конфіденційної інформації. У сучасних умовах, коли обсяги обробки даних зростають, а цифрові загрози стають все більш складними, системи шифрування

набувають критичної важливості для збереження цілісності та конфіденційності податкової інформації.

Серед основних організаційних заходів – регулярна зміна паролів, обмеження доступу до інформації на основі посадових обов'язків, та ведення журналів аудиту [33, с.120].

Серед найбільш використовуваних алгоритмів шифрування для забезпечення безпеки податкової інформації слід виділити симетричне та асиметричне шифрування. Симетричне шифрування використовує один і той самий ключ для шифрування та дешифрування даних. Це може бути ефективним при передачі великих обсягів даних, проте його основним обмеженням є необхідність забезпечення безпеки ключа, оскільки його компрометація може призвести до втрати цілісності всієї системи. Асиметричне шифрування використовує пару ключів — один публічний (для шифрування) і один приватний (для дешифрування). Цей метод є більш надійним, оскільки навіть якщо публічний ключ доступний, без приватного ключа дані залишаються захищеними.

Стандарт рекомендує створення централізованої системи управління доступом з використанням ролей для розмежування рівнів доступу до даних [34, с.25].

Крім того, для посилення захисту передавання даних застосовуються протоколи безпечної передачі інформації, такі як SSL/TLS, які забезпечують захищену комунікацію між користувачем і сервером, гарантуючи, що передані дані не будуть перехоплені або змінені під час транспортування.

Особливу увагу також слід приділяти захисту даних, які зберігаються на сервері або в інших сховищах інформації. Використання шифрування для збереження даних гарантує, що навіть у разі фізичного доступу до серверів, доступ до чутливої інформації буде заблоковано без відповідних засобів дешифрування. Це стає ще важливішим в умовах високих ризиків, пов'язаних із зовнішніми атаками або несанкціонованим доступом всередині організації.

Найбільш перспективними для використання в податкових органах є такі інструменти шифрування, як алгоритми AES (Advanced Encryption Standard) для симетричного шифрування, а також RSA (Rivest-Shamir-Adleman) для асиметричного шифрування. Вони є стандартами міжнародного рівня, підтримуються на практиці багатьма державами та організаціями, що забезпечує міждержавну сумісність і високий рівень захисту інформації.

Інтеграція систем автоматизованого виявлення аномалій і поведінкової аналітики дозволяє попереджати більшість сучасних атак [35, с.89].

Системи багатофакторної автентифікації (БФА) стали важливим елементом сучасної системи захисту інформації, оскільки вони дозволяють значно підвищити рівень безпеки при доступі до чутливих даних, зокрема до податкової інформації. БФА включає в себе використання кількох незалежних рівнів перевірки особи, що значно ускладнює доступ до системи для несанкціонованих осіб і знижує ризики витоку даних через компрометацію лише одного рівня безпеки.

Основним принципом БФА є поєднання декількох факторів, що перевіряються під час авторизації користувача. Зазвичай такі фактори поділяються на три основні категорії: щось, що знає користувач (наприклад, пароль або PIN-код), щось, що має користувач (наприклад, токен або мобільний телефон), і щось, що є властивим користувачу (наприклад, біометричні дані, такі як відбитки пальців або розпізнавання обличчя).

Перше рівня перевірки — це те, що знає користувач. Традиційно це був пароль або PIN-код, які використовуються для ідентифікації особи.

Другим рівнем є щось, що має користувач, наприклад, фізичний пристрій, такий як мобільний телефон або спеціальний апаратний токен.

Третій рівень — це щось, що є властивим користувачу, і це найсучасніший та найнадійніший спосіб підтвердження особи. Біометричні методи, такі як розпізнавання обличчя, відбитки пальців або сканування райдужної оболонки ока, надають ще один рівень захисту, оскільки такі дані є унікальними для кожної людини.

Застосування БФА для доступу до податкової інформації дозволяє забезпечити багатоступеневу перевірку, що робить несанкціонований доступ значно складнішим і менш імовірним.

Наприклад, в податкових органах БФА може застосовуватися для доступу до системи електронних декларацій, де платники податків та інші користувачі повинні пройти кілька етапів перевірки перед тим, як отримати доступ до особистої або фінансової інформації. Перший етап може включати введення пароля, другий — введення одноразового коду, надісланого на мобільний телефон або електронну пошту, а третій — підтвердження особи через біометричні дані, такі як відбиток пальця або розпізнавання обличчя.

Хмарні технології та штучний інтелект стають ключовими інструментами у сфері інформаційної безпеки, дозволяючи реагувати на загрози у реальному часі [36, с.250].

Водночас важливою складовою для успішної реалізації БФА є регулярне оновлення та вдосконалення систем безпеки.

Антивірусні та антипоштові системи відіграють важливу роль у захисті інформаційних систем від шкідливих програм, які можуть бути використані для несанкціонованого доступу до податкової інформації. В умовах сучасного розвитку технологій і збільшення кількості кіберзагроз, ефективний захист від вірусів, троянів, програм-вимагачів та іншого шкідливого програмного забезпечення стає критично важливим для забезпечення безпеки даних.

Антивірусні системи є першою лінією оборони для будь-якої інформаційної інфраструктури, оскільки вони виявляють та блокують шкідливі програми, що можуть потрапити в систему через різноманітні канали, такі як електронна пошта, веб-сайти, зовнішні пристрої збереження даних (флешки, зовнішні жорсткі диски) тощо. Вони активно сканують файли, програми та інші елементи системи, порівнюючи їх із відомими підписами шкідливого програмного забезпечення в своїх базах даних. При виявленні загрози антивірусна програма може або заблокувати, або видалити

заражений файл, що допомагає запобігти проникненню шкідливих елементів у систему.

Крім традиційних антивірусних засобів, важливу роль в захисті даних відіграють антипоштові системи. Вони спрямовані на захист від спаму, фішингу, а також більш складних атак через електронну пошту, таких як розповсюдження шкідливих програм, які маскуються під легітимні повідомлення. Фішингові атаки часто використовують підроблені листи, які схожі на офіційні повідомлення від податкових органів, щоб заманити користувача і змусити його перейти за посиланням або завантажити заражений файл. Антипоштові фільтри аналізують вхідні електронні листи за кількома критеріями: домен, зміст листа, наявність підозрілих вкладень або посилань, і негайно блокують листи, які відповідають критеріям загрози.

Моніторинг та виявлення вторгнень є ключовими складовими частинами системи безпеки в захисті податкової інформації. З огляду на те, що інформаційні системи податкових органів обробляють великі обсяги конфіденційних даних, таких як фінансова інформація платників податків, доступ до цих систем повинен бути строго контролюваним, а будь-які спроби несанкціонованого доступу — негайно виявлені та нейтралізовані. Для цього використовуються спеціалізовані інструменти та методи моніторингу активності, які дозволяють своєчасно виявити підозрілі дії та загрози в системах.

Сучасні правила передбачають обов'язкове використання криптографічних засобів захисту при передачі податкових даних між системами [37, с.18].

Одним із основних підходів до забезпечення моніторингу є встановлення систем виявлення вторгнень (IDS — Intrusion Detection Systems) та систем попередження про вторгнення (IPS — Intrusion Prevention Systems). Системи IDS активно аналізують всі дії, що відбуваються в інформаційних мережах та на серверах, з метою виявлення аномальних або шкідливих дій, які можуть вказувати на спробу несанкціонованого доступу. Вони працюють

на основі різних методів, таких як порівняння поточної активності з попередньо встановленими підписами відомих загроз (метод підписів) або на основі поведінкового аналізу, що дозволяє виявляти нові, невідомі загрози (метод аномалій). У разі виявлення підозрілої активності, система одразу генерує попередження або ініціює певні дії, щоб запобігти вторгненню, наприклад, блокування доступу до системи або ізоляцію порушеного сегмента мережі.

Щоб забезпечити ще більш високий рівень безпеки, моніторинг системи може бути доповнений використанням інтегрованих платформ для управління подіями та інцидентами безпеки (SIEM — Security Information and Event Management). Ці платформи об'єднують дані з різних джерел — систем IDS, журналів доступу, мережевих пристроїв, серверів та інших компонентів інфраструктури, — і забезпечують централізовану обробку та аналіз. Вони дозволяють не лише оперативно виявляти та реагувати на інциденти, а й зберігати історію подій для подальшого аналізу і визначення потенційних вразливостей в системі.

Резервне копіювання та відновлення даних є критично важливими складовими системи захисту інформації, особливо у випадку обробки конфіденційних та стратегічно важливих даних, таких як податкова інформація. Системи резервного копіювання забезпечують збереження даних у випадку технічних збоїв, зловмисних атак або людських помилок, що є непередбачуваними ризиками в сучасному інформаційному середовищі. Відновлення даних після інцидентів є процесом, який дозволяє повернути систему до робочого стану і мінімізувати втрати важливої інформації.

Основною метою резервного копіювання є створення точних, актуальних копій даних, які можна відновити в разі їх втрати або пошкодження. Залежно від рівня критичності інформації, копії даних можуть зберігатися на різних носіях, таких як жорсткі диски, сервери, оптичні носії або навіть хмарні платформи. Резервне копіювання може бути організовано на кількох рівнях, зокрема на рівні окремих файлів, баз даних чи цілих

систем. Важливим є регулярне виконання резервного копіювання, що гарантує актуальність копій, особливо для даних, які постійно змінюються, таких як податкові декларації, звіти та інші фінансові документи.

Зазначену процедуру слід регулярно тестувати через симуляцію реальних ситуацій відновлення, щоб переконатися в її ефективності та зменшити ймовірність помилок при відновленні. Тестування відновлення має бути частиною плану безпеки та виконуватися з певною періодичністю, оскільки технології змінюються, а старі методи можуть стати непридатними. Кожен етап відновлення — від визначення джерела резервної копії до фактичного поновлення даних — має бути задокументований, а відповідальні особи повинні бути чітко визначені.

Розробка і впровадження чітких політик доступу та контролю є необхідним кроком у забезпеченні надійного захисту податкової інформації. У сучасних умовах, коли інформація є однією з найбільш цінних ресурсів, правильне управління доступом до неї стає критично важливим для запобігання несанкціонованому доступу, витоку даних і зловживань. Основним принципом політик доступу є принцип "необхідності знати", який передбачає, що доступ до податкової інформації надається лише тим особам, які безпосередньо потребують цієї інформації для виконання своїх службових обов'язків.

Перш за все, розробка політики доступу починається з чіткого визначення, які дані є чутливими, а які — загальнодоступними. У контексті податкової інформації це можуть бути дані про доходи платників податків, фінансові звіти, декларації та інша інформація, що стосується діяльності підприємств та фізичних осіб. Визначення цих даних дозволяє розробити політики доступу таким чином, щоб мінімізувати можливість несанкціонованого доступу до найбільш чутливих категорій інформації.

Важливим елементом будь-якої політики доступу є чітке визначення санкцій за порушення правил доступу та захисту інформації. Співробітники, які не дотримуються політик або намагаються зловживати доступом, повинні

нести відповідальність, що може включати дисциплінарні заходи, штрафи або навіть кримінальне покарання в разі серйозних порушень. Такі санкції повинні бути прописані в політиці доступу та доведені до відома всіх співробітників для забезпечення належного контролю за їх дотриманням.

Розробка політики доступу — це лише перший крок. Для її ефективного впровадження необхідно провести регулярні тренінги та навчання для співробітників, які працюють з податковою інформацією. Це допомагає не лише покращити розуміння політики доступу, а й підвищити обізнаність про можливі загрози та ризики. Співробітники повинні знати, чому важливо обмежувати доступ до чутливої інформації і як це сприяє забезпеченню її безпеки.

Розробка і впровадження чітких політик доступу є критично важливим етапом у захисті податкової інформації. Принцип "необхідності знати", що є основним у таких політиках, допомагає мінімізувати ризики несанкціонованого доступу і забезпечити безпеку даних. Однак, для ефективної реалізації цих політик необхідно створити чіткі процедури надання і скасування доступу, моніторити його використання та впроваджувати санкції за порушення. Тільки за допомогою комплексного підходу можна забезпечити належний рівень захисту податкової інформації, що є важливим не лише для держави, а й для збереження довіри громадян до податкової системи.

Навчання та підвищення кваліфікації персоналу — це не одноразова акція, а постійний процес, що має на меті створення професійної та відповідальної команди, здатної ефективно реагувати на всі виклики, що виникають у сфері захисту податкової інформації. Таким чином, правильна організація навчання та постійне підвищення кваліфікації співробітників є важливим етапом у системі захисту інформації, оскільки дозволяє не лише знижувати ризики, а й значно покращувати загальний рівень безпеки в організації.

Розробка внутрішніх інструкцій та протоколів є невід'ємною частиною системи безпеки при обробці та зберіганні податкової інформації. Ці інструкції виконують роль фундаментальних документів, які визначають порядок дій співробітників та організаційні процедури в процесі роботи з конфіденційними даними. Основною метою створення таких внутрішніх стандартів є забезпечення надійного та ефективного захисту податкової інформації від несанкціонованого доступу, витоків або змін, що можуть призвести до порушення законодавства або зниження довіри до податкових органів.

Важливим аспектом є також передбачення заходів, які повинні бути вжиті для відновлення захисту інформації після порушення. Це включає в себе відновлення доступу тільки тим особам, які мають відповідні повноваження, а також перевірку і посилення політик безпеки, щоб подібні порушення не повторювались у майбутньому. Окрім того, важливо визначити, чи повинні бути проведені додаткові тренінги для персоналу або оновлені методи контролю доступу, щоб зменшити ймовірність повторення інцидентів.

Інноваційні рішення, такі як біометрія та багатофакторна автентифікація, демонструють значну ефективність у попередженні несанкціонованого доступу до конфіденційних даних [38, с.16].

Отже, технологічні засоби захисту та організаційні заходи для запобігання несанкціонованому доступу до податкової інформації є основними елементами ефективної системи безпеки в умовах постійно зростаючих кіберзагроз. Впровадження сучасних технологій, таких як шифрування даних, системи моніторингу та виявлення вторгнень, а також використання автентифікаційних процедур на кількох рівнях, дозволяє суттєво знизити ризики несанкціонованого доступу до конфіденційної інформації. Разом з тим, важливу роль у забезпеченні безпеки відіграють організаційні заходи, серед яких належне управління доступом до даних, розробка політик безпеки та навчання співробітників. Комбінація

технологічних і організаційних заходів створює надійний бар'єр для потенційних загроз і сприяє збереженню цілісності та конфіденційності податкової інформації.

РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ ПОДАТКОВОЇ ІНФОРМАЦІЇ

3.2. Інноваційні технології та розробки сучасного забезпечення для захисту податкової інформації.

Інноваційні технології мають значний вплив на забезпечення захисту податкової інформації. У сучасному цифровому середовищі, де інформація обробляється та передається в великих обсягах, ефективний захист даних стає критично необхідним. Основними технологічними інструментами для забезпечення безпеки податкової інформації є системи шифрування, біометричні та мультифакторні методи автентифікації, інтелектуальні системи виявлення загроз, блокчейн-технології, хмарні рішення для зберігання та обробки даних, а також новітні засоби захисту від кіберзагроз.

Використання новітніх алгоритмів шифрування є основною ланкою забезпечення захисту податкової інформації від несанкціонованого доступу в умовах цифровізації [39].

Зміни в законодавстві, у своїй кваліфікаційній роботі я звертаю увагу на деякі прогалини в українському законодавстві щодо захисту податкової інформації. Одним із основних аспектів, який потребує вдосконалення, є законодавче визначення правового режиму податкової інформації. Закон України "Про захист персональних даних" і Податковий кодекс України вимагають уточнення в частині обробки та збереження податкової інформації, а також заходів для протидії її несанкціонованому доступу.

По-перше, необхідно чітко визначити правові механізми, які б забезпечували захист податкової інформації на всіх етапах її обробки — від збору та зберігання до передачі та використання. Наприклад, в Податковому кодексі України не вказані конкретні вимоги щодо умов та форм доступу до податкової інформації, що могло б ускладнити захист персональних даних платників податків. Я вважаю, що варто внести зміни, які б зобов'язували державні органи забезпечити суворіші контрольні заходи при доступі до

таких даних, зокрема шляхом впровадження мультифакторної автентифікації для співробітників, які працюють з податковими даними.

По-друге, важливо посилити санкції за порушення вимог щодо захисту податкової інформації. Законодавство має бути більш конкретним у визначенні відповідальності за несанкціоноване використання, передачу або поширення таких даних. Внесення змін у частину Кодексу про адміністративні правопорушення дозволить створити більш ефективну систему покарань для тих, хто порушує конфіденційність податкової інформації.

Також вважаю, що в частині надання доступу до податкової інформації необхідно запровадити більш чіткі правила, що базуються на принципі необхідності знати. Це дозволить обмежити коло осіб, які можуть отримувати доступ до таких даних, знижуючи ризик їхнього зловживання або витоку.

Окремо необхідно звернути увагу на міжнародні стандарти та норми, адже українське законодавство не завжди враховує найновіші розробки у сфері технологій та інновацій, що стосуються захисту персональних даних. Важливо запровадити законодавчі ініціативи, що забезпечать відповідність нормам європейського регламенту GDPR та інших міжнародних стандартів безпеки.

Згідно зі статтею 35 Закону України "Про захист персональних даних", "особа, яка обробляє персональні дані, зобов'язана забезпечити їх захист від несанкціонованого доступу, знищення, змін, блокування, копіювання, поширення, а також від інших неправомірних дій щодо персональних даних" (Закон України "Про захист персональних даних", 2010). Однак, на мою думку, в даному законі не достатньо чітко регламентовані вимоги щодо захисту податкової інформації, що є однією з найбільш чутливих категорій даних. Тому необхідно внести зміни, що уточнять механізми захисту податкових даних і визначатимуть конкретні вимоги до безпеки доступу до цієї інформації.

Також відповідно до частини 3 статті 65 Податкового кодексу України, "податкові органи зобов'язані забезпечити конфіденційність податкової інформації, що містить відомості про платників податків" (Податковий кодекс України, 2010). Вважаю, що це положення потребує уточнення щодо технологічних і організаційних заходів, що повинні впроваджуватися для запобігання витоку даних і несанкціонованому доступу до податкової інформації.

Використання криптографії для захисту податкової інформації забезпечує високий рівень конфіденційності даних, що має вирішальне значення для запобігання їх витоку [40, с.45-55].

Інтелектуальні системи виявлення загроз, що базуються на штучному інтелекті та машинному навчанні, стають все більш популярними у захисті податкової інформації. Вони дозволяють в реальному часі аналізувати дані, виявляти аномалії та своєчасно реагувати на потенційні загрози. Такі системи здатні адаптуватися до нових типів атак, прогнозувати можливі порушення і надавати оперативні рішення для мінімізації ризиків.

Блокчейн-технології дозволяють забезпечити прозорість та незмінність податкової інформації, що значно знижує ризики фальсифікацій і маніпуляцій з даними [41, с.112-115].

Блокчейн-технології використовуються для забезпечення прозорості та цілісності податкових даних. Завдяки своїй здатності забезпечити незмінність записів і прозорість процесів, блокчейн гарантує, що інформація не може бути змінена або видалена без відома всіх учасників. Це робить блокчейн ідеальним для забезпечення надійного захисту податкових даних, зокрема для збереження записів про транзакції та податкові декларації.

Блокчейн забезпечує високий рівень безпеки, дозволяючи здійснювати запис транзакцій без можливості їх зміни, що надзвичайно важливо для захисту податкових даних [42, с.33-38].

Останнім, але не менш важливим напрямом є розробка нових засобів захисту від кіберзагроз. Протидія новітнім хакерським атакам, таких як

фішинг, вірусні атаки чи інші форми кіберзлочинності, вимагає використання передових технологій. Регулярне оновлення програмного забезпечення, застосування нових алгоритмів для виявлення загроз і швидке реагування на інциденти дозволяють зберігати високий рівень безпеки податкової інформації.

Інноваційні технології відіграють ключову роль у сучасному забезпеченні захисту податкової інформації. В умовах цифровізації суспільства, коли все більше даних передається та зберігається в електронному вигляді, питання забезпечення конфіденційності, цілісності та доступності податкової інформації набуває особливої важливості. Стрімкий розвиток технологій створює нові можливості для забезпечення більш ефективного захисту даних, проте також виникають нові виклики та загрози, зокрема в сфері кібербезпеки.

Однією з основних причин, чому інноваційні технології стали необхідними в контексті захисту податкової інформації, є значне зростання обсягів даних, що обробляються органами податкової служби. Це вимагає надійних і масштабованих рішень, здатних забезпечити високий рівень захисту при одночасному збереженні швидкості обробки інформації. Сучасні системи шифрування, а також біометричні та мультифакторні технології автентифікації дозволяють значно підвищити рівень захисту даних, забезпечуючи належний контроль доступу до чутливої податкової інформації.

Штучний інтелект здатний здійснювати постійний моніторинг активності в інформаційних системах та оперативно виявляти підозрілі дії, що суттєво підвищує рівень захисту податкової інформації [43, с.78-84].

Ще одним важливим аспектом є інтеграція інтелектуальних систем для виявлення загроз. Технології на основі штучного інтелекту та машинного навчання дають змогу в реальному часі виявляти спроби несанкціонованого доступу до систем та вчасно реагувати на потенційні загрози. Такі системи здатні аналізувати величезні обсяги даних, виявляючи аномальні патерни поведінки, які можуть свідчити про спроби порушення безпеки.

Крім того, важливим напрямком є використання хмарних технологій для зберігання та обробки даних. Хмарні рішення надають високу гнучкість, масштабованість і доступність ресурсів, що дозволяє органам податкової служби оперативно реагувати на зміну обсягів інформації, що обробляється. При цьому, хмарні технології можуть бути забезпечені додатковими засобами захисту, такими як автоматичне шифрування даних та регулярні аудити безпеки, що робить їх важливим інструментом для забезпечення захисту податкової інформації.

Хмарні технології дозволяють зберігати великі обсяги податкових даних з високим рівнем безпеки, а також забезпечують доступ до них лише уповноваженим особам.[44, с.110-115].

Новітні алгоритми шифрування дозволяють досягти високого рівня безпеки, запобігаючи доступу до даних навіть у разі перехоплення їх під час передачі через незахищені канали зв'язку. Одним із таких алгоритмів є алгоритм асиметричного шифрування, зокрема протокол RSA, що широко використовується для захисту даних у системах електронних платежів і обміну податковими даними. В основі цього методу лежить пара ключів: відкритий і закритий. Відкритий ключ використовується для шифрування інформації, а закритий — для її дешифрування. Цей метод гарантує, що тільки уповноважені особи, які володіють відповідним закритим ключем, можуть розшифрувати дані.

Іншим важливим інструментом у сучасних системах шифрування є симетричні алгоритми, такі як AES (Advanced Encryption Standard). Вони використовують один і той самий ключ для шифрування та дешифрування інформації. AES є одним з найбільш потужних і швидких методів шифрування, і його застосування забезпечує високий рівень безпеки при обробці великих обсягів даних. Завдяки ефективності цього алгоритму він широко використовується для шифрування даних в комунікаційних системах, зокрема в електронних системах податкового обміну, де необхідно

забезпечити конфіденційність фінансової та особистої інформації платників податків.

З нових досягнень у галузі криптографії можна відзначити так звану квантову криптографію, яка, хоча й перебуває на етапі розвитку, може стати важливим кроком у забезпеченні безпеки даних у майбутньому. Квантові комп'ютери, які здатні обробляти величезні обсяги даних, можуть порушити нинішні стандарти криптографії, тому вчені активно працюють над створенням нових квантових алгоритмів шифрування, які будуть захищати дані навіть від потужних квантових атак. Технологія квантового шифрування використовує принципи квантової механіки для забезпечення непередбачуваності та незмінності даних, що робить її надзвичайно надійною для захисту чутливої інформації.

Крім того, однією з новітніх розробок є використання гібридних методів шифрування, які поєднують різні типи алгоритмів для досягнення максимального рівня безпеки. Це може бути, наприклад, комбінація асиметричного шифрування для обміну ключами і симетричного для швидкої передачі великих обсягів даних. Такі методи зменшують ймовірність успішного нападу на інформацію, оскільки навіть якщо один алгоритм буде зламаний, інші залишатимуться захищеними.

Інноваційні засоби захисту, такі як біометричні технології, гарантують не тільки конфіденційність, а й автентичність доступу до податкової інформації [45, с.119-124].

Біометричні та мультифакторні технології автентифікації стали важливими інструментами для забезпечення високого рівня безпеки при доступі до чутливої інформації, включаючи податкові дані. В умовах зростаючих кіберзагроз, особливо в таких сферах, як оподаткування, захист персональних та фінансових даних потребує застосування складних методів ідентифікації користувачів. Біометрія та багаторівнева автентифікація дозволяють значно підвищити надійність систем безпеки, мінімізуючи ризики несанкціонованого доступу.

Мультифакторні методи автентифікації забезпечують додатковий рівень безпеки, що дозволяє уникнути несанкціонованого доступу до конфіденційної податкової інформації [46, с. 61-65].

Багаторівнева автентифікація не є абсолютно неприступною. Вона вимагає постійного оновлення та вдосконалення в умовах розвитку нових технологій кіберзагроз. Тому важливо забезпечити не лише впровадження таких систем, а й регулярне тестування їх ефективності, вдосконалення алгоритмів, а також підтримку актуальності баз даних біометрії, щоб захист податкової інформації залишався на найвищому рівні.

Таким чином, біометричні та багаторівневі технології автентифікації є одними з найефективніших методів захисту податкової інформації, адже вони забезпечують максимальний рівень безпеки, підтверджуючи особистість користувача за допомогою унікальних фізіологічних або поведінкових ознак, а також доповнюючи їх іншими факторами. Це дозволяє суттєво знизити ризики несанкціонованого доступу до чутливої інформації та забезпечити її цілісність і конфіденційність.

Інтелектуальні системи виявлення загроз, що базуються на штучному інтелекті (ШІ) та машинному навчанні, набувають все більшої популярності в контексті захисту податкової інформації. Ці технології дозволяють здійснювати більш ефективний моніторинг безпеки в реальному часі та швидко реагувати на потенційні загрози, що з'являються у складних та динамічних умовах сучасних інформаційних систем.

Основна перевага використання ШІ в контексті захисту податкової інформації полягає в тому, що він здатен обробляти величезні обсяги даних за короткий час і виявляти аномалії, які можуть вказувати на несанкціоновані дії або загрози. Системи ШІ можуть аналізувати поведінку користувачів та активність в інформаційних системах, виявляючи відхилення від нормальних патернів, що можуть свідчити про спроби атаки або зловмисний доступ до чутливої інформації.

Машинне навчання, яке є складовою частиною ІІІ, дозволяє системам безпеки навчатися на основі попередніх інцидентів і з часом ставати більш ефективними у виявленні нових типів загроз. Це досягається за рахунок алгоритмів, що автоматично адаптуються до нових ситуацій та постійно вдосконалюються. Наприклад, якщо система ІІІ раніше виявила порушення безпеки, машинне навчання може використати цей досвід для створення нових моделей поведінки користувачів та системи в цілому. Це дозволяє виявляти навіть раніше невідомі загрози, які можуть бути виявлені лише за допомогою глибокого аналізу великих обсягів даних.

Інтелектуальні системи виявлення загроз за допомогою машинного навчання дозволяють своєчасно виявляти аномалії, які можуть свідчити про спроби несанкціонованого доступу [47, с.50-54].

Одним із ключових аспектів роботи інтелектуальних систем виявлення загроз є їх здатність до самооптимізації. Технології, що застосовуються для виявлення аномалій, використовують різноманітні алгоритми для прогнозування можливих загроз. Наприклад, система може оцінювати ймовірність того, що певна дія користувача є шкідливою, на основі зібраних даних про попередні інциденти безпеки та поведінкові патерни. Якщо система зафіксувала незвичну активність, таку як кілька спроб введення неправильного пароля або надмірний доступ до великих обсягів даних в короткий проміжок часу, вона може сигналізувати про можливу загрозу або ініціювати автоматичне блокування доступу до інформаційних ресурсів.

Інтелектуальні системи можуть також виявляти нові загрози, не спираючись лише на попередній досвід або вже визначені шаблони атак. Наприклад, системи на базі ІІІ можуть виявляти раніше невідомі уразливості в програмному забезпеченні, оцінюючи потенційні ризики і пропонуючи стратегії для їх усунення. Машинне навчання дозволяє цим системам адаптуватися до змін в інфраструктурі або поведінці користувачів, що дає змогу оперативно реагувати на нові типи атак.

Одним із практичних застосувань таких систем є їх інтеграція з іншими елементами інфраструктури безпеки. Наприклад, інтелектуальні системи можуть поєднуватися з системами моніторингу в режимі реального часу або системами управління інцидентами для автоматичного реагування на загрози. Таке поєднання дозволяє значно підвищити ефективність реакції на кіберзагрози, зменшуючи час між виявленням загрози та її нейтралізацією.

Враховуючи складність і постійно змінювану природу кіберзагроз, інтелектуальні системи, що базуються на ШІ та машинному навчанні, надають необхідний рівень гнучкості та адаптивності для боротьби з ними. Ці системи не лише допомагають виявляти відомі загрози, але й здатні передбачати нові варіанти атак, що робить їх незамінними інструментами для забезпечення безпеки податкової інформації в умовах сучасних кіберзагроз.

Хмарні технології, які раніше вважалися лише інноваційним інструментом для зберігання даних та виконання обчислень, сьогодні стали невід'ємною частиною інфраструктури безпеки у багатьох сферах, зокрема в обробці та захисті податкової інформації. Це явище, що активно розвивається, передбачає використання віддалених серверів для зберігання, обробки і передачі даних через інтернет, замість традиційного використання локальних серверів або фізичних носіїв інформації. Такий підхід має значний потенціал для покращення якості і безпеки податкових систем, що обробляють чутливі дані.

Однією з головних переваг хмарних рішень є зручність доступу до даних з будь-якої точки світу, що дає можливість миттєво реагувати на зміни або інциденти в обробці податкової інформації. Однак, ключовим аспектом, який робить хмарні технології особливо привабливими для захисту податкових даних, є їх здатність забезпечити більш високий рівень безпеки в порівнянні з традиційними локальними методами зберігання.

Одним з інших важливих аспектів хмарних рішень є їх здатність до автоматичного масштабування. Зі збільшенням обсягів оброблених даних хмарні сервіси здатні без проблем додавати додаткові ресурси, що дозволяє

забезпечити безперервність і високу ефективність обробки податкової інформації. У цьому контексті хмара допомагає не лише забезпечити необхідний рівень безпеки, але й ефективно справлятися з великими обсягами даних, що характерно для сучасних податкових систем.

Хмарні сервіси також відкривають нові можливості для інтеграції з іншими національними та міжнародними системами обміну податковою інформацією. Оскільки хмарні технології забезпечують стандартизовані та безпечні канали для обміну даними, вони дозволяють державам і компаніям легко інтегрувати свої податкові системи, сприяючи прозорості та оперативному обміну інформацією, що є важливим аспектом у боротьбі з податковими шахрайствами.

Наостанок, варто зазначити, що хмарні рішення для зберігання та обробки податкових даних можуть істотно зменшити витрати на інфраструктуру і технічне обслуговування. Оскільки обробка і зберігання даних відбувається на віддалених серверах, організаціям більше не потрібно інвестувати значні кошти в локальні сервери, їх обслуговування або оновлення. Цей аспект робить хмарні технології особливо привабливими для державних установ та великих корпорацій, які прагнуть знизити свої витрати на інфраструктуру.

У сучасному світі, де інформаційні технології стали основою економіки та державного управління, захист від кіберзагроз є пріоритетним завданням для всіх секторів, зокрема для податкових органів. Кіберзагрози, що постійно еволюціонують, створюють нові виклики для забезпечення безпеки даних, зокрема податкової інформації, яка є особливо чутливою і може стати об'єктом різноманітних атак. Тому розробка нових засобів захисту від кіберзагроз та хакерських атак є не лише технічним завданням, а й необхідністю для підтримки довіри до податкової системи.

Одним із основних напрямків розробки нових засобів захисту є постійне вдосконалення технологій шифрування. Шифрування залишається одним з найефективніших методів захисту даних від несанкціонованого доступу.

Однак, у міру розвитку обчислювальних потужностей та зростання здатностей зломисників до розшифрування, існуючі алгоритми шифрування можуть бути не достатньо захищеними. Тому сучасні системи шифрування повинні інтегрувати новітні алгоритми, які використовують квантові методи шифрування або інші передові математичні принципи, щоб гарантувати безпеку навіть у випадку появи нових способів атаки.

Ще одним критичним напрямом є розробка нових систем виявлення і запобігання вторгнень (IDS/IPS), які повинні забезпечувати своєчасне виявлення спроб несанкціонованого доступу до систем. У світі кіберзагроз, що постійно змінюються, необхідні такі системи, які здатні швидко адаптуватися до нових типів атак, зокрема до складних, багатофазних атак, які часто маскуються під легітимний трафік. Використання штучного інтелекту та машинного навчання дозволяє таким системам не лише реагувати на вже відомі загрози, а й передбачати можливі атаки, аналізуючи поведінку мережевих пристроїв і виявляючи аномалії, які можуть свідчити про майбутнє вторгнення.

Одним з найбільш серйозних викликів є захист від атак типу "деніал-оф-сервіс" (DDoS), які можуть паралізувати роботу критично важливих інформаційних систем. Відповідно, в розробці нових засобів захисту особливу увагу слід приділяти створенню систем, здатних автоматично розпізнавати та нейтралізувати такі атаки. Це можуть бути як апаратні засоби захисту, так і програмні алгоритми, що розподіляють навантаження та блокують підозрілу активність у реальному часі, зберігаючи при цьому стабільність і доступність сервісів.

Протидія сучасним кіберзагрозам та хакерським атакам вимагає постійного оновлення методів захисту та впровадження новітніх технологій у сфері безпеки інформації [48, с.104-108].

Незамінними в контексті протидії новітнім кіберзагрозам є також технології блокчейн. Використання блокчейн-технологій для зберігання та обміну даними гарантує незмінність і цілісність інформації. Ці технології

дозволяють створювати дистрибутивні реєстри, що унеможливлюють спроби змінити або підробити податкові дані без виявлення змін. Відкритість і прозорість блокчейн-мереж знижує ризик шахрайства і зловживань, забезпечуючи високий рівень захисту від атак.

Крім цього, новітні методи аутентифікації, такі як біометричні технології або багатофакторна автентифікація, стають все більш важливими в контексті кіберзахисту. Використання одночасно декількох рівнів перевірки особи, таких як відбитки пальців, розпізнавання обличчя або голосу, значно знижує ймовірність несанкціонованого доступу до систем. Важливим аспектом є також інтеграція таких методів з новими протоколами безпеки, які дають змогу перевіряти не тільки ідентичність користувача, але й його поведінку в системі, що дозволяє виявляти потенційно небезпечні зміни в патернах доступу.

Крім технологічних засобів захисту, необхідно розробляти нові стандарти і методології для моніторингу та аудиту інформаційних систем. Аудит безпеки має стати невід'ємною частиною повсякденної діяльності кожної організації, яка працює з чутливою податковою інформацією. Регулярні перевірки на відповідність стандартам безпеки, виявлення та усунення вразливостей систем є критично важливими для своєчасного виявлення загроз і запобігання можливим атакам.

Особливу увагу слід приділяти навчанню і підвищенню кваліфікації співробітників, оскільки навіть найкращі технічні засоби не зможуть ефективно захистити від кіберзагроз, якщо користувачі не будуть дотримуватись правил безпеки. Тому розробка ефективних тренінгів та підвищення обізнаності персоналу є важливою складовою стратегії протидії кіберзагрозам.

Загалом, протидія новітнім кіберзагрозам і хакерським атакам вимагає комплексного підходу, який включає впровадження інноваційних технологій, постійне оновлення та адаптацію засобів захисту, а також інтеграцію нових методів управління безпекою та навчання персоналу. Урахування цих

факторів дозволить забезпечити надійний захист податкової інформації від всіх можливих загроз, сприяючи стабільності та ефективності роботи податкових органів у цифрову епоху.

Отже, інноваційні технології та розробки сучасного забезпечення для захисту податкової інформації відіграють ключову роль у забезпеченні надійності та безпеки даних в умовах цифровізації та постійного зростання кіберзагроз. Впровадження новітніх технологій, таких як блокчейн, штучний інтелект, багаторівнева автентифікація та хмарні рішення, дозволяє значно підвищити рівень захисту інформації, зменшити ризики несанкціонованого доступу та забезпечити прозорість та ефективність податкових процесів. Розвиток інструментів для захисту податкової інформації не тільки забезпечує високий рівень конфіденційності, але й сприяє підвищенню довіри між державою, платниками податків та іншими зацікавленими сторонами. Тому впровадження інноваційних технологій в податкову сферу є необхідною умовою для ефективного функціонування системи оподаткування в умовах сучасних викликів.

ВИСНОВКИ

У результаті проведеного дослідження нами сформульовано наступні висновки, спрямовані на досягнення поставленої мети.

Захист податкової інформації є критично важливим для забезпечення фінансової безпеки держави, оскільки податкові надходження становлять основну частину доходів бюджету. Відсутність належного захисту податкової інформації може призвести до серйозних фінансових втрат і загроз для національної безпеки країни. Крім того, в умовах зростаючих кіберзагроз, підвищена увага до цього питання є невідкладною.

Сучасні інноваційні технології, такі як криптографія, біометричні системи та штучний інтелект, здатні значно посилити захист податкової інформації, забезпечуючи високу надійність і конфіденційність даних, що обробляються податковими органами. Використання цих технологій може зробити систему захисту більш гнучкою та адаптованою до нових викликів, таких як кібератаки і несанкціонований доступ.

Правова регламентація інноваційних технологій для захисту податкової інформації в Україні потребує подальшого вдосконалення. Зокрема, існує необхідність адаптації національних законодавчих актів до міжнародних стандартів, що забезпечать ефективну боротьбу з кіберзагрозами. Важливою складовою цього є створення умов для співпраці з міжнародними організаціями в рамках обміну досвідом і запровадження передових практик у сфері кібербезпеки.

Для забезпечення ефективного захисту податкової інформації важливо запровадити новітні технології та інструменти, які будуть відповідати вимогам сучасних загроз і відповідати потребам держави у фінансовій стабільності та економічному розвитку. Такий підхід дозволить не тільки підвищити рівень безпеки, а й сприятиме створенню довіри серед платників податків до системи державного управління.

Інноваційні технології не лише підвищують рівень безпеки, але й можуть сприяти підвищенню ефективності податкової політики та адміністрування, а також зміцненню фінансової безпеки держави, забезпечуючи надійний захист податкових надходжень і зниження рівня тіньової економіки. Це дозволяє створити сприятливі умови для розвитку економіки та поліпшення рівня життя населення.

Важливим є не лише впровадження новітніх технологій, але й постійне їх оновлення та адаптація до змінюваних умов інформаційної безпеки. Зі швидким розвитком технологій кіберзагроз, існує необхідність у створенні гнучкої системи оновлень, яка дозволить податковим органам оперативно реагувати на нові виклики безпеки. Включення таких процесів в національну стратегію кібербезпеки є необхідним кроком для забезпечення стабільного і безпечного функціонування податкової системи.

Крім того, важливо забезпечити взаємодію між державними органами, приватним сектором та міжнародними організаціями у сфері захисту податкової інформації. Така співпраця дозволить створити спільні механізми для боротьби з кіберзагрозами та покращити обмін інформацією між державами, знижуючи ймовірність виникнення транснаціональних кіберзлочинів.

На додаток до правових і технологічних аспектів, важливу роль у захисті податкової інформації відіграє культурний і організаційний рівень державних установ. Створення корпоративної культури, яка підвищує обізнаність працівників податкових органів про важливість збереження конфіденційності даних, є важливою складовою успіху в загальній боротьбі за захист інформації. Навчання працівників з питань інформаційної безпеки та забезпечення обізнаності щодо ризиків допоможе мінімізувати потенційні загрози з боку внутрішніх джерел.

Останнім аспектом є необхідність впровадження системи зворотного зв'язку та оцінки ефективності заходів із захисту податкової інформації. Створення механізмів для постійного аудиту і ревізії політик безпеки

дозволить своєчасно виявляти недоліки в існуючих системах захисту та покращувати їх. Важливо, щоб ці заходи були інтегровані в регулярні процеси контролю та вдосконалення безпеки в органах державної податкової служби.

Враховуючи важливість розробки та впровадження інноваційних технологій, необхідно провести реформи в законодавстві та системі управління податковими даними, що відповідають сучасним вимогам безпеки. Тільки за умови комплексного підходу до цієї проблеми можна забезпечити стабільний захист податкової інформації та зберегти фінансову безпеку країни на високому рівні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- 1.Іваненко, О. М. Правові аспекти захисту податкової інформації. Київ: Юрінком Інтер, 2020., 256 с.
- 2.Коваленко, Т. І. Конфіденційність податкової інформації в Україні: правові та організаційні аспекти. Вісник податкової служби України, 2019, № 6, 10-15 с.
- 3.Smith, J. Tax Information Protection and Legal Privacy Concerns. Oxford University Press, 2018., 320 p.
- 4.Кравченко, О. В. Правові основи захисту інформації в Україні. Київ: Наукова думка, 2021., 304 с.
5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 33. Ст. 304. Дата оновлення 28.06.2024 URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (звернення 20.12.2024)
6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 32. Ст. 481. Дата оновлення 19.21.2024 URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення 20.12.2024)
7. Про затвердження Порядку захисту інформації в інформаційно-комунікаційних системах органів державної податкової служби: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. Офіційний вісник України. 2006. № 14. С. 798–802. Дата оновлення 21.10.2022 URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF> (звернення 20.12.2024)
- 8.Ковальчук, І. В. Інформаційне право України. Харків: Право, 2021., 320 с.
- 9.Шевчук, В. М. Правове регулювання податкової інформації в Україні. Київ: Юридична література, 2020. 256 с.

10.Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. Дата оновлення 15.11.2024 URL:<https://zakon.rada.gov.ua/laws/show/2657-12> (звернення 20.12.2024)

11.Податковий кодекс України : Закон України від 02.12.2010 р. № 2755-VI. Відомості Верховної Ради України. 2011. № 13-14, № 15-16, № 17. Ст. 112. Дата оновлення 01.01.2025 URL:<https://zakon.rada.gov.ua/laws/show/2755-17> (звернення 05.01.2025)

12.Про порядок доступу до інформаційних ресурсів податкових органів : наказ Державної податкової служби України від 10.03.2021 р. № 56. Офіційний вісник України. 2021. № 23. С. 56. Дата оновлення 05.06.2023 URL:<https://zakon.rada.gov.ua/laws/show/z0946-23#Text> (звернення 20.12.2024)

13.Пилипенко, В. Г. Актуальні проблеми правового регулювання інформаційної діяльності в Україні. Київ: Юрінком Інтер, 2018., 380 с.

14.Звіт Рахункової палати України за 2023 рік. Київ : Рахункова палата України, 2023. 12 с. (звернення 05.01.2025)

15.Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

16.Ковальчук, І. В. Інформаційна безпека в податковій сфері. Київ: Видавничий дім "Юрінком Інтер", 2021., 157 с.

17.Розслідування Державної податкової служби України, 2022 р.-9 с.

18.Горбач, О. П. Правове забезпечення захисту податкової інформації. Львів: Центр наукової літератури, 2020. 312 с.

19.Звіт Національного центру кібербезпеки України за 2023 рік. Київ : НЦКБ, 2023. 16 с. Дата оновлення 05.06.2023 URL:<https://scpsc.gov.ua/uk/articles/334> (звернення 20.12.2024)

20.Про затвердження заходів із захисту інформаційних ресурсів : наказ Державної податкової служби України від 15.03.2021 р. № 87. Офіційний вісник України. 2021. № 23. С. 4. Дата оновлення 14.06.2024 URL:<https://zakon.rada.gov.ua/laws/show/z0593-20#Text> (звернення 20.12.2024)

- 21.Горбач, О. П. Правове забезпечення захисту податкової інформації. Львів: Центр наукової літератури, 2020. 312 с.
- 22.Ковальчук, І. В. Інформаційна безпека в податковій сфері. Київ: Видавничий дім "Юрінком Інтер", 2021. 284 с.
- 23.Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286. Дата оновлення 28.06.2024 URL:<https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (звернення 20.12.2024)
- 24.Про затвердження заходів із захисту інформаційних ресурсів : наказ Державної податкової служби України від 15.03.2021 р. № 87. Офіційний вісник України. 2021. № 23. 112–114 с. Дата оновлення 14.06.2024 URL:<https://zakon.rada.gov.ua/laws/show/z0593-20#Text> (звернення 20.12.2024)
- 25.Національний стандарт України ДСТУ 8302:2015 "Захист інформації. Загальні принципи побудови інформаційної безпеки". Київ : Держстандарт України, 2015. 45 с.
- 26.Рекомендації Європейської організації з кібербезпеки (ENISA) щодо захисту податкових даних. Брюссель : ENISA, 2022. 38 с.
- 27.Звіт Національного центру кібербезпеки України за 2023 рік. Київ : Національний центр кібербезпеки України, 2023. 16 с.
- 28.Горбач, О. П. Інформаційна безпека у фінансовій сфері. Львів: Центр наукової літератури, 2020. 320 с.
- 29.Ковальчук, І. В. Організаційні заходи кіберзахисту: основи та методи. Київ: Юрінком Інтер, 2021. 276 с.
- 30.Національний стандарт України ДСТУ 8825:2021 "Інформаційна безпека. Захист критичних інформаційних ресурсів". Київ : Національний орган стандартизації, 2021. 24 с.
- 31.Шевченко, М. О. Інформаційно-аналітичні системи: безпека та захист даних. Харків: Видавництво ХНУ, 2022., 298 с.

32. Про заходи із захисту інформації в інформаційно-телекомунікаційних системах: Наказ Державної податкової служби України від 15.03.2021 № 98. Офіційний вісник України. 2021. № 10. С. 45–47.

33. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою: ДСТУ ISO/IEC 27001:2015 Київ: Держстандарт України, 2015. 120 с.

34. Рекомендації Європейської організації з кібербезпеки (ENISA) щодо захисту податкових даних. Брюссель: Європейська організація з кібербезпеки, 2022. 25 с.

35. Рекомендації Європейської організації з кібербезпеки (ENISA) щодо захисту податкових даних. Брюссель: Європейська організація з кібербезпеки, 2022. 89 с.

36. Смірнов, А. В. Технологічні інновації у сфері захисту даних. Одеса: ОНУ, 2022. 250 с.

37. Правила доступу до інформаційних систем : Державний стандарт України затверджено 2023 року. Київ: Держстандарт України, 2023. 18 с.

38. Звіт Національного центру кібербезпеки України за 2023 рік. Київ: Національний центр кібербезпеки України, 2023. 16 с.

39. Трофимова, С. А. Теоретико-правові аспекти захисту інформації в Україні: монографія. Київ: Інтертех, 2020. С. 98-102.

40. Петров, І. М. Роль криптографії у захисті податкової інформації в Україні. Журнал з кібербезпеки., 2020. №3. С. 45-55

41. Герасимчук, Л. О. Інформаційна безпека в умовах цифровізації: підручник. Львів: Академія, 2021. С. 112-115.

42. Міхеєва, І. М. Блокчейн та новітні технології для забезпечення безпеки податкової інформації. Право та інновації. 2019. №6. С. 33-38.

43. Загородня, І. В. Перспективи використання штучного інтелекту для захисту даних. Інформаційні технології у праві. 2021. №4. С. 78-84.

44.Луценко, Т. С. Хмарні технології для зберігання та захисту податкової інформації: міжнародний досвід та українська практика. Юридичний журнал. 2020. № 10. С. 110-115.

45.Дмитриченко, О. О. Розвиток інноваційних засобів захисту податкової інформації в Україні. Харків: Наука, 2020. С. 119-124.

46.Іванова, Л. О. Впровадження багаторівневої автентифікації для захисту інформації у податкових органах. Вісник юридичних наук. 2021. №2. С. 61-65.

47.Чернишова, І. В. Інтелектуальні системи виявлення загроз для захисту податкової інформації. Технічні аспекти безпеки даних. 2020. №7. С. 50-54.

48.Коваленко, М. В. Інноваційні методи захисту податкової інформації: теорія та практика. Київ: Юрінком Інтер, 2022. С. 104-108.