діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра фінансів. Державна фіскальна служба відповідно до покладених на неї завдань контролює своєчасність подання платниками податків та єдиного внеску передбаченої законом звітності, своєчасність, достовірність, повноту нарахування та сплати податків і зборів, єдиного внеску, митних та інших платежів [3].

Отже, в Україні сформовано цілісну систему державного фінансового контролю як сукупність контрольно-аналітичних і експертних дій органів зовнішнього та внутрішнього державного фінансового контролю за суб'єктами державного сектора з метою забезпечення законності, запобігання порушенням фінансової дисципліни, економічної ефективності під час формування, розподілу й використання державних фінансових ресурсів.

Підсумовуючи вищезазначене, можна зробити висновок, що у сучасних умовах розвитку ринкових відносин в Україні, які супроводжуються процесами поширення корупції та проявами шахрайства в бюджетній сфері, пов'язаними із привласненням бюджетних коштів в особливо великих розмірах, виникає об'єктивна необхідність у забезпеченні дієвості державного фінансового та правоохоронного контролю, який би сприяв законності та раціональності використання коштів і майна, що належать державі.

Варто звернути увагу й на те, що у різних органів державного фінансового контролю в Україні однакові повноваження та підконтрольні об'єкти. Водночас потенційне дублювання функцій контролюючих органів повинне розглядатися як система стримувань і противаг, що забезпечить принцип прозорості державного фінансового контролю.

1. Ангеліна І. А. Система органів державного фінансового контролю і нагляду України: проблеми формування.. *Економічний часопис XXI.* 2013. № 11-12. С. 95-98.
2. Дніпрова Т. Доброчесність, відповідальність, достовірність – три базові цінності американської системи державного фінансового контролю. *Фінансовий контроль*. 2017. № 5. С.13-17.
3. Дребот С. Європейський вектор у сфері перебудови системи державного фінансового контролю. *Фінансовий контроль*. 2015. № 2. С. 42-47.
4. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. Київ: Просвіта, 1996. 80 с. (із наступними змінами та доповненнями).
5. Бюджетний кодекс України від 08.07.2010. *Відомості Верховної Ради України.* 2010, № 50-51. Ст. 572.

Сергій ПРОКОПОВ
старший викладач кафедри
економічної та інформаційної безпеки
Катерина БУЦАНОВА
студентка ННІ права та інноваційної
освіти Дніпропетровського державного
університету внутрішніх справ
(м. Дніпро, Україна)

ПРОБЛЕМИ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Сучасна інформаційна безпека сьогодні дуже важлива для всіх, хто користується комп'ютером або будь-яким гаджетом, які використовуються у повсякденній діяльності. Це майже всі. Інформаційна безпека має бути в центрі уваги кожного, оскільки велика частина нашої особистої інформації знаходиться в Інтернеті. Науковці стверджують, що інформаційна безпека необхідна через ризик, який виникає, коли технологія використовується для обробки інформації, оскільки інформація може бути розкрита неправильним чином або не тій людині. Багато компаній і організацій, які лише працюють із щоденними даними, вживають усіх запобіжних заходів щоб запобігти хакерам спричиняти атаки та зловживання даними, використовуючи системи виявлення та запобігання вторгненням, маніпулятори, а також відповідне навчання та політику, яку впроваджують їхні менеджери з безпеки. Але якщо говорити про соціальні мережі, це інша гра в м'яч. Служби соціальних мереж (SNS), як-от Facebook або Instagram, не є такими безпечними, незважаючи на технології, запроваджені на їхніх підприємствах, або політику, встановлену їхнім персоналом безпеки. Основною причиною цього є інформація, яку

користувачі розміщують у цих соціальних мережах[1].

Приголомшлива популярність цих соціальних мереж, якими часто користуються підлітки та люди, у яких немає конфіденційності чи безпеки, призводить до розміщення величезної кількості потенційно приватної інформації в Інтернеті, де інші можуть мати до нього доступ. Вся інформація, яку люди публікують на цих сайтах з роками, перетворюється на колекцію інформації, яка стає відомою, наприклад як ваш профіль, і майже будь-хто в мережі може бачити її, особливо ваші друзі. Таким чином, із постійним поширенням в соціальних мережах різного роду інформації існує постійний ризик для безпеки, але не в основному з боку хакерів чи злодіїв, а через помилкову довіру, яку багато людей мають.

Обмін інформацією та спілкування з людьми існує відтоді, як люди існують. Але коли комп'ютери та Інтернет стали більш поширеними, почалось використання систем електронної пошти та коротких текстових повідомлень як перший популярний засіб спілкування між людьми. Це було не так небезпечно, оскільки передбачало надсилання одного повідомлення за раз між двома людьми, і це було не більш ризикованим, ніж надсилання іншої інформації через Інтернет лише одній людині. Але наука не стоїть на місці, тому далі з'явилося більше технологій, таких як чати та онлайн-ігри, а потім і соціальні мережі, де користувачі могли ділитися інформацією, говорити, обговорювати інтереси та уподобання, публікувати фотографії та відео тощо. Одним із перших подібних соціальних мереж був MySpace. Його оригінальною аудиторією були підлітки та музично-художня сцена. Його популярність як скеля впала, коли Facebook з'явився в мережі, а потім він став найпопулярнішою соціальною мережею[2].

Основним ризиком конфіденційності та безпеки інформації в соціальних мережах є централізована архітектура. Сервери соціальних мереж — це золота копальня особистої інформації, від якої вільно відмовляються як підлітки, так і дорослі користувачі. Це викликає серйозні занепокоєння щодо конфіденційності та може призвести до таких речей, як крадіжка особистих даних та продаж даних користувача третім сторонам. Користувачі мають хибне почуття довіри до свого провайдера соціальних мереж, щоб захистити свою інформацію, коли вона часто продається третім особам або зламана зрадниками особистих даних. Але хоча Facebook додав налаштування конфіденційності, якими може керувати користувач, їх налаштування за замовчуванням є загальнодоступними. Таким чином, новий користувач, який не змінює ці налаштування, щоб зробити їх більш суворими, насправді публікує інформацію, яку можуть переглядати громадськість і не друзі. Кількість інформації, яку довірливі користувачі розміщують у своїх профілях на популярних сайтах соціальних мереж, можна зібрати разом, щоб сформувати зображення користувача. Зловмисник може створити фальшивий профіль цієї особи, знову подружитися з усіма їхніми друзями, а потім обманом змусити своїх друзів розкрити більше особистої інформації про користувача. Називає цю практику «клонуванням профілю». Деякі злодії крадуть інформацію про користувачів з одного сайту, щоб створити фейковий профіль на іншому. Також інформацію можна вилучити з користувачів за допомогою фішингових атак, коли інформацію отримують від користувачів за допомогою створення підроблених вебсайтів, які запитують особисту інформацію або навіть паролі та номери соціального страхування. Різні інші атаки розроблені для того щоб або отримати особисту інформацію користувачів, або заражати їх систему вірусами [3].

Найбільша проблема тут полягає в тому, що багато користувачів не знають про налаштування конфіденційності та способи їх використання. Вони також «не знають про ризики, пов'язані із завантаженням конфіденційної інформації». Дослідження показали, що сайти соціальних мереж створені для того, щоб об'єднати якомога більше користувачів в одному місці. Ці сайти цінують «відкритість, зв'язок і обмін з іншими – на жаль, саме ті аспекти, які дозволяють кіберзлочинцям використовувати ці сайти як зброю для різних злочинів».

Щоб уникнути потенційної втрати приватної та особистої інформації, слід розібратися в розумінні цих ризиків і проблем. Кількість опублікованої особистої інформації має бути обмежена, не публікувати домашні адреси чи особисту контактну інформацію. Також подумайте про Інтернет як про загальнодоступний. Будьте скептичними і остерігайтеся незнайомців. Не кожен є тим, за кого себе видає, і вони могли вкрасти чиюсь особистість, щоб здійснити кіберзлочин. Не користуйтеся стороннімі програмами, які часто зустрічаються у Facebook. Вони часто встановлюють шкідливе програмне забезпечення, яке відстежує вашу діяльність в Інтернеті. Використовуйте надійні паролі, антивірусне

програмне забезпечення. За тими, у кого є діти, за ними потрібно дуже уважно стежити, оскільки вони часто не знають мудрих методів онлайн-безпеки або не піклуються про те, щоб захистити себе. Пам'ятайте, що після того, як ви публікуєте щось, воно ніколи не зникає, навіть якщо ви його видалите.

Найбільшою проблемою тут є необережність у тому, що публікують в Інтернеті, і це одна з найпростіших для концептуального вирішення. Можливе рішення, безсумнівно, не є повним, але допоможе розв'язати проблему та зменшити кількість недбалості в Інтернеті, а також вписується в ідею використання освіти як одного з трьох способів захисту інформаційних систем. Пропонується, щоб усі соціальні мережі, включаючи Facebook, Instagram, Twitter, Flickr, LinkedIn, а також усі портативні програми, що мають подібну мету, пропонували вимагати від усіх нових користувачів під час реєстрації в обліковому записі переглянути коротке відео, в якому обговорюється тема безпеки в Інтернеті, особиста інформація та інструкції щодо налаштувань конфіденційності цієї мережі. Кнопка для подання облікового запису не повинна з'являтися, доки відео не відтвориться. Таким чином, його неможливо обійти, як юридичні застереження, які люди просто приймають сліпо. Крім того, будь-які поточні користувачі повинні будуть переглянути відео в день його виходу в Інтернет, щоб продовжувати використовувати свої облікові записи[4].

З усього цього досить ясно, що соціальні мережі становлять великий ризик для безпеки та конфіденційності. У них є такий ризик через їх централізовану архітектуру, величезне сховище всієї особистої інформації, і загальне незнання населення щодо того, як правильно використовувати налаштування конфіденційності для підвищення безпеки в Інтернеті. Найкраще, що ми можемо зробити, це бути розумними в Інтернеті. Але з кращою освітою та деякими архітектурними змінами соціальні мережі можна використовувати безпечніше. Освіта – це найбільша частина. Люди впадають у самовдоволення і іноді їм потрібно нагадувати про речі. Нарешті, важливо продовжити дослідження щодо того, як зробити соціальні мережі більш безпечними, навіть якщо довірливі користувачі розміщують в Інтернеті безліч особистої інформації.

1. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. Вип. 24. С. 252-262.
2. Мельник К. С. Обробка та захист персональних даних в соціальних мережах. *Інформація і право*. 2014. №. 3. С. 64-69.
3. Москаленко М. В. Захист інформації в соціальних мережах. *Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 23-25 листоп. 2016 р.)*. Кропивницький : КНТУ, 2016. С. 143-144.
4. Черниш Р. Соціальні мережі як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності.* 2017. Вип. 136. С. 205-214.

Ігор КРІЦАК
аспірант кафедри адміністративного
та господарського права Запорізького
національного університету
(м. Запоріжя, Україна)

МЕДІАЦІЯ ЯК ФОРМА ДОСУДОВОГО ВРЕГУЛЮВАННЯ АДМІНІСТРАТИВНО-ПРАВОВИХ СПОРІВ

Судове вирішення будь-яких публічно-правових спорів в адміністративних судах є останнім етапом врегулювання спірних правовідносин. Однією, і сьогодні основною формою досудового або позасудового вирішення публічно-правових спорів є медіація – позасудова процедура врегулювання конфлікту (спору), яка здійснюється за допомогою (посередництвом) медіатора як спеціально підготовленої нейтральної, незалежної, неупередженої фізичної особи, яка проводить медіацію.

Наразі можливість врегулювання публічно-правового спору в позасудовому (медіаційному) порядку з'явилась у зв'язку з прийняттям та набуттям чинності Закону України «Про медіацію» від 16 листопада 2021 року № 1875-IX (далі – Закон) [1]. У зв'язку з тим що процедура медіації в публічно-правових спорах набула нормативного урегулювання, нижче доцільно визначити основні положення щодо участі медіатора у