

**Дацюк В.Б.,**  
кандидат юридичних наук,  
керівник юридичного департаменту  
ІТ-Корпорації «ТРАНСОФТГРУПА»

## РОЗДІЛ 4

### ІТ-ПРАВО ТА ЕКОНОМІЧНІ СВОБОДИ

#### 4.1. Економіко-правовий аналіз поняття ІТ-права та сфери його застосування

Сфера застосування інформаційних технологій спричинила появу специфічної, раніше невідомої людству сфери суспільних відносин – відносин у цифровому (віртуальному) просторі, а з ними й формування високотехнологічної та високоприбуткової галузі економіки. Це об'єктивно зумовлює необхідність належного правового регулювання такого роду економічних відносин на рівні такої ж специфічної та комплексної галузі права як ІТ-право. Для України вказане питання актуальне як ніколи, адже за останніми дослідженнями вітчизняний ринок послуг у сфері інформаційних технологій набирає дедалі більших обертів та станом на сьогодні створює близько 4% ВВП. При цьому у 2018 році комп'ютерні послуги стали другою в країні найбільшою галуззю з експорту послуг (після переробки товарів), випередивши навіть трубопровідний транспорт. Більше того, за експертними висновками темпи загального зростання ІТ-галузі в Україні становлять близько 20% щороку та випереджають навіть загальносвітовий показник (6-7%). У свою чергу сума сплачених вітчизняними ІТ-компаніями податків у 2014–2017 роках зростала щороку у середньому на 27% і у 2018 році досягла 10 млрд грн<sup>1</sup>.

Стабільно зростає й кількість ІТ-спеціалістів, яка за останні кілька років збільшилася майже на 60% - зі 100 тис. у 2016 році до 161 тис. станом на початок 2019 року. На додаток до цієї цифри слід врахувати, що згідно з даними Опендатабот в категорії «Комп'ютерне програмування, консультування та пов'язана з ними діяльність» зареєстровано 129,5 тисяч підприємців. Також підприємці реєструються в категоріях: «Видання іншого програмного забезпечення», «Консультування з питань інформатизації», «Видання комп'ютерних ігор», «Оброблення даних та розміщення інформації на веб-вузлах». Загалом з 2017 по 2019 роки кількість ФОП в ІТ-сфері зросла на 40 676 ІТ-підприємців, тобто на 45%. При цьому їх частка серед інших фізичних осіб-підприємців зросла з 5% до 7,5%<sup>2</sup>. Втім вражають не лише кількісні, а й якісні показники вітчизняного ринку ІТ-спеціалістів. Так, згідно з даними, що були опубліковані у звіті про стан європейської технічної індустрії State of European Tech, у 2018 році в Україні налічувалося 184 700 професійних розробників програмного

---

<sup>1</sup> Підгайна, Є., 2018. Пішли на прорив: український ІТ-ринок зростає швидше за світовий, *Mind*. [online] Відновлено з: <https://mind.ua/publications/20189963-pishli-na-proriv-ukrayinskij-it-rinok-zrostaе-shvidshe-za-svitovij> ІТ-індустрія в 2018 р. сплатить близько 10 млрд грн податків, *Інформаційне агентство «Інтерфакс-Україна»*. Відновлено з: <https://ua.interfax.com.ua/news/economic/541529.html>

<sup>2</sup> Опендатабот, 2019. Чому законопроект про ФОП може нашкодити саме ІТ-бізнесу? [online] Відновлено з: <https://opendatabot.ua/blog/294-jesuis-fop>

забезпечення. Це дозволило Україні увійти у першу десятку країн Європи за кількістю таких фахівців<sup>3</sup>. При цьому ще у 2014 році Україна опинилася на четвертому місці у світовому рейтингу країн за кількістю сертифікованих ІТ-спеціалістів (після США, Індії, Росії), а також увійшла до основних тридцяти місць розташування для передавання замовлень на розроблення програмного забезпечення<sup>4</sup>.

Вказане свідчить про стрімкий розвиток ІТ-сектору економіки України. Хоче хтось того чи ні, інформаційні технології стали невід'ємною частиною нашого життя (як в роботі, так і у побуті), а у розрізі сучасної світової економіки ІТ-галузь є однією з найперспективніших та такою, що стрімко розвивається і видозмінюється, створює нові й нові можливості не лише для ІТ-спеціалістів, але й для представників інших професій та спеціальностей, що так чи інакше дотичні до сфери ІТ або обслуговують цю галузь (вчені, інженери, менеджери, юристи, економісти тощо). Відтак важливо, щоб законодавство та практика правозастосування встигали за такими тенденціями розвитку сучасних економічних відносин, враховуючи їх особливу специфіку, а не перетворювалися на фактор гальмування ІТ-бізнесу, зокрема, та економічного зростання, в цілому.

Про формування ІТ-права в Україні як самостійної галузі права (з точки зору усталених у вітчизняній науці підходів до поділу системи права на галузі за предметом та методом правового регулювання), на наш погляд, говорити зарано. Хоча сучасні вчені-юристи уже почали напрацьовувати предмет, систему та методологію ІТ-права. Однак при цьому нерідко застосовується вузький підхід. Зокрема Є.О. Харитонов у 2016 році визначив ІТ-право як сукупність норм та правил, що опосередковують діяльність по *забезпеченню безпеки інформаційних технологій та інформаційної активності в мережі Інтернет*<sup>5</sup>. Згодом вчений дещо переглянув та уточнив своє визначення ІТ права як *відносно визначеної сукупності норм та правил, що опосередковують діяльність щодо забезпечення реалізації інформаційних технологій та інформаційної активності в мережі Інтернет*<sup>6</sup>. Останнє визначення, на наш погляд, є більш наближеним до специфіки ведення бізнесу у сфері ІТ, який аж ніяк не обмежується лише безпекою інформаційних технологій, а стосується різних аспектів правових та економічних відносин, пов'язаних із створенням, обслуговуванням, тестуванням програмних продуктів, передачею прав на них тощо.

Вітчизняний вчений А.В. Новицький характеризує норми права, що регулюють суспільні відносини в ІТ-сфері України, теж застосовує досить вузький підхід та констатує такі види формування правових норм: а) ті, що склалися історично (ЗУ «Про інформацію»); б) ті, що були прийняті на вимогу світової спільноти (ЗУ «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг»; в) ті, що прийняті на вимогу розвитку індустрії (ЗУ «Про Національну програму інформатизації»)<sup>7</sup>. В додаток до наведеної

---

<sup>3</sup> Wehmeier, Tom and the Atomico Team, 2018. State of European Tech Report. [online] Available at: <https://2018.stateofeuropeantech.com/chapter/europes-got-talent/article/people-power/>

<sup>4</sup> Винничук, Р.О., Склярчук, Т.В., 2015. *Особливості розвитку ІТ-ринку в Україні: стан та тенденції*. Вісник Національного університету "Львівська політехніка", Логістика, № 833, С. 3-8. [online] Режим доступу: [http://nbuv.gov.ua/UJRN/VNULPL\\_2015\\_833\\_3](http://nbuv.gov.ua/UJRN/VNULPL_2015_833_3)

<sup>5</sup> Харитонов, Є.О. (2016). Сутність ІТ-права (ІТ-право як концепт). *Збірник матеріалів науково-практичної конференції «ІТ право: проблеми і перспективи розвитку в Україні»*. Львів, НУ «Львівська політехніка», с.274.

<sup>6</sup> Харитонов, Є.О., Харитонova О.І., 2017. Поняття ІТ-права, сфера його дії та структура. Т.В. Бачинський (Ред.), *Основи ІТ-права*, Київ, Юрінком Інтер, с.7-22.

<sup>7</sup> Новицький, А.В. (2016). *Місце ІТ-права в загальній системі інформаційного права*. Збірник матеріалів науково-практичної конференції «ІТ право: проблеми і перспективи розвитку в Україні», Львів, НУ «Львівська політехніка», С.116.

класифікації можна також виділити ще один вид правових норм – ті, що прийняті для захисту інформаційної безпеки, як складової національної безпеки України (ЗУ «Про правові засади забезпечення кібербезпеки України»). Однак і у такому вигляді наведена класифікація відобразатиме далеко не всі аспекти відносин, які склалися у практиці ведення ІТ-бізнесу.

Більш прогресивною у своїх поглядах є О.С. Яворська, яка говорить про ІТ-право як *про право цифрового середовища* та зазначає, що йдеться не про якесь особливе право, а насамперед *про специфіку функціонування, застосування та прояву правових норм щодо суспільних відносин в особливому середовищі, яким і є цифрове середовище*. Саме така специфіка, на думку вченої, й відрізняє ІТ-право від інформаційного права, хоча чисто граматично ці поняття співпадають. При цьому вчена зауважує, що усталені в науці галузеві підходи, в основі яких предмет і метод правового регулювання, попри свою користь у контексті системного пізнання права в рамках навчального процесу все ж створюють штучні перепони на шляху до розв'язання практичних проблем, зокрема й тих, що стосуються визначення поняття та місця ІТ-права в сучасній системі права<sup>8</sup>. І справді – сформулювати предмет та метод ІТ-права, визначити його чітке місце у системі права досить складно. З точки зору усталених наукових підходів до структурування системи права, ІТ-право уже давно вийшло за рамки міжгалузевого правового інституту, але ще не «виросло» у самостійну галузь права в класичному її розумінні. Та й чи доцільно виводити таку галузь, штучно «прищеплюючи» до неї частини цивільного господарського, адміністративного, трудового та інших класичних галузей права? Однак об'єктивне існування ІТ-права як галузі практики сьогодні абсурдно заперечувати.

Варто також звернутися до особливостей визначення дефініції ІТ-права у західній юриспруденції. Так, на правовому інформаційному порталі HG.org, який є дискусійним майданчиком для юристів США, наведене таке пояснення сутності права інформаційних технологій (ІТ-права) як нішевої практики:

*«ІТ-право забезпечує правову базу для збору, зберігання та розповсюдження електронної інформації на глобальному ринку. Адвокати, які практикують у цій галузі права, представляють фізичних осіб та підприємства різних галузей. Вони допомагають структурувати транзакції з інформаційними технологіями таким чином, щоб максимально збільшити економічну вигоду клієнта, одночасно забезпечуючи дотримання регуляторних норм. Великий акцент робиться також на передбаченні потенційних джерел спорів між сторонами угоди та на розробці угод, які вирішують ці проблеми, тим самим зменшуючи ризик судових процесів.*

*Коли виникають суперечки в галузі інформаційних технологій, які не можуть бути вирішені поза судовою системою, юрист, що спеціалізується на таких видах справ, може виявитись більш потужним фахівцем порівняно із юристом загальної спеціалізації. Юридичні фірми із практикою у сфері ІТ-права працевлаштовують юристів, що мають практичний досвід роботи в цій галузі ще до вступу в юридичну професію. З огляду на це, адвокат є більш ефективним у поясненні технічних понять судді чи присяжним, і, швидше за все, матиме контакти в галузі, які роблять пошук консультантів та експертів менш складним»<sup>9</sup> (пер. з англ. – В.Д.).*

<sup>8</sup> Яворська, О.С., 2017. *ІТ-право*, Львів, Вид-во «Левада», С.10-16.

<sup>9</sup> Information Technology Law, Guide to IT Law. HG.org Legal Resources. [online] Available at: <https://www.hg.org/information-technology-law.html#1>

Відтак варто зазначити, що у західній юриспруденції ІТ-право здебільшого розглядається не як самостійна галузь права у класичному її розумінні, а як галузь практики, яка стосується різних правових аспектів стосовно договорів у сфері інформаційних технологій, інтелектуальної власності, конфіденційності та захисту інформації тощо<sup>10</sup>.

В сучасній вітчизняній та зарубіжній юридичній літературі можна також знайти такі терміни як Інтернет-право, комп'ютерне право, кіберправо, правова інформатика тощо. Однак, на наш погляд, ІТ-право є найбільш влучним поняттям, яке включає у себе усі вище перелічені, та стосується відносин у віртуальному середовищі як з використанням мережі Інтернет, так і без такої, але з використанням інформаційних технологій (наприклад, створення автономних баз даних без підключення до мережі Інтернет).

На нашу думку, ІТ-право сьогодні слід розглядати у першу чергу як галузь практики, яка виникла і розвивається незалежно від волі законодавця та становить собою сукупність норм різних галузей законодавства, які так чи інакше регулюють специфічні відносини, що складаються у сфері інформаційних технологій. Не дарма практикуючі юристи говорять про правове обслуговування ІТ-бізнесу як про окрему індустрію (галузь) юридичної практики. Відтак ІТ-право як індустрія в праві охоплює такі аспекти правового забезпечення ІТ-сфери як:

- 1) правовий супровід стартапів в ІТ-сфері;
- 2) вибір юрисдикції та реєстрація ІТ-бізнесу;
- 3) договірні відносини, електронна комерція та ЗЕД-контракти у сфері ІТ;
- 4) податкове структурування ІТ-бізнесу;
- 5) питання щодо антимонопольного права в ІТ-секторі;
- 6) особливості валютного регулювання та банківських відносин у сфері ІТ;
- 7) трудові відносини в ІТ-компаніях;
- 8) реєстрація авторських прав та реєстрація знаків для товарів та послуг;
- 9) захист персональних даних;
- 10) правове забезпечення кібербезпеки;
- 11) правова допомога у вирішенні конфліктів в ІТ-сфері (досудове та судове врегулювання спорів) тощо.

Суттєвим фронтом для ІТ-юристів є впровадження **комплаєнс-стандартів** у роботі з іноземними контрагентами (насамперед, із компаніями зі США та ЄС), виходячи з вимог міжнародно-правового регулювання та з урахуванням специфіки зарубіжних правових систем. Більш детально мова про це піде у параграфі, присвяченому особливостям юридичного супроводу ІТ-бізнесу в Україні в умовах глобалізації.

Враховуючи взаємозв'язок економічних та правових процесів, також відзначимо, що правовий супровід ІТ-бізнесу в Україні за останній час став ще й доволі прибутковою справою для нішевих юристів. Тобто ІТ-право не лише покликане обслуговувати ІТ-бізнес, але й саме по собі є перспективною сферою ведення юридичного бізнесу. У зв'язку із цим ІТ-право можна розглядати у двох аспектах:

- 1) **з точки зору права** - як **галузь практичної юриспруденції** для всіх юристів, які мають стосунок до ІТ-сфери, зокрема:
  - корпоративних юристів (інхаусів) ІТ-підприємств;

---

<sup>10</sup> Michalsons, 2018. What is IT law, ICT law or Cyber law? [online] Available at: <https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286>

- адвокатів, а також юристів інших підприємств, установ, організацій (державних і недержавних), які в ході роботи стикаються з питаннями правового регулювання ІТ-відносин;

2) **з точки зору економіки - як *бізнес-індустрію* для:**

- зовнішніх юристів (зокрема й адвокатів), які займаються вузькоспеціалізованою приватною практикою у сфері обслуговування ІТ-бізнесу;
- нішевих юридичних компаній, що здійснюють правовий супровід ІТ-підприємств (наприклад, Legal IT Group (м. Київ);
- юридичних компаній, які мають у своїй структурі відповідні підрозділи, що надають консалтингові послуги у сфері ІТ (наприклад, Юридична фірма «AEQUO» (м.Київ), Адвокатське об'єднання «Бачинський та партнери» (м.Львів) та інші).

Підсумовуючи викладене значимо, що наведений нами перелік складових ІТ-сфери, які формують своєрідний предмет правового регулювання ІТ-права (якщо все ж вдаватися до цих категорій), не претендує на свою вичерпність. До того ж ми визнаємо свій чітко виражений бізнес-підхід до розуміння сутності та призначення ІТ-права. Так, поза нашою увагою залишилися такі питання як Інтернет речей, штучний інтелект та інші новації сучасного суспільства, які є результатом стрімкого розвитку інформаційних технологій та які сьогодні піддаються аналізу вчених, у тому числі з точки зору права. Поле для досліджень правовідносин в ІТ-сфері є доволі широким та розширюється, без перебільшення, з кожним днем. Тож залишимо відповідні аспекти для подальших, більш ґрунтовних науково-практичних досліджень, присвяченим конкретним аспектами правового регулювання ІТ-відносин.

#### **4.2. Свобода підприємництва та реалізація права на працю в ІТ-сфері: вітчизняні контраверсії**

Ні для кого не секрет, що застаріле трудове законодавство є одним із гальмівних та ризикових чинників розвитку ІТ-бізнесу в Україні. Вітчизняне законодавство не передбачає особливих умов щодо оформлення трудових відносин для окремих сфер господарської діяльності чи для представників малого підприємництва. Гострою проблемою для ІТ-компаній є відсутність можливості застосувати нетрадиційні конструкції в трудових договорах, які не передбачені в Кодексі законів про працю України. При цьому трудове законодавство України досить суворе: статтею 9 КЗпП обмежено свободу сторін у визначенні умов, адже умови договорів, які погіршують становище працівників, є недійсними (а це, наприклад, покладання додаткових обов'язків, установлення додаткових обмежень, відповідальності тощо)<sup>11</sup>. Окрім того вітчизняне законодавство досі невизначене в питаннях *фрілансу*, що уже давно став звичною практикою в ІТ-галузі. Питання впровадження гнучкого графіку робочого часу передбачені не законом та навіть не підзаконним актом, а Методичними рекомендаціями щодо встановлення гнучкого режиму робочого часу, затвердженими наказом Мінпраці України від 04.10.2006 № 359.

---

<sup>11</sup> Яценко, Т., 2019. Особливості оформлення трудових відносин в ІТ-компаніях і стартапах: теорія та практика. *ЮРИСТ&ЗАКОН*, №41, 14 листопада

В питаннях офіційного оформлення трудових відносин вітчизняні ІТ-компанії стикаються з проблемою формування власного штатного розкладу, виходячи із посад, передбачених Класифікатором професій ДК 003:2010. Так, сучасні ІТ-спеціалісти звикли до таких загальнозживаних у світі вакансій як «Front-End Developer», «Back-End Developer», «Software Tester», «QA Engineer» тощо, які відображають вузьку специфіку тієї чи іншої роботи в ІТ-сфері. Натомість українські айтішники змушені влаштовуватися на посади «Програміст прикладний», «Програміст системний», «Інженер-програміст», «Програміст (база даних)» специфіка та різниця між якими не зовсім зрозуміла, а формулювання такої посади як «Фахівець із розробки та тестування програмного забезпечення» (тобто програміст та тестувальник в одній особі) взагалі виглядає абсурдно. Варто відзначити, що сам Класифікатор професій є документом, що має доволі сумнівну природу, адже затверджений наказом Держспоживстандарту України від 28.07.2010 № 327, однак не зареєстрований в Міністерстві юстиції України. У той же час необхідність використання Класифікатора передбачена Інструкцією про порядок ведення трудових книжок працівників. А тому ігнорування Класифікатора професій може спричинити несприятливі наслідки для роботодавця у вигляді накладення штрафу при проведенні перевірки Держпраці.

Над нюансами пострадянської практики укладення трудових правовідносин, а також ведення кадрової документації можна не замислюватися, якщо заключити з ІТ-спеціалістом цивільно-правовий договір, особливо якщо він має статус фізичної-особи підприємця. Переваги роботи із фізичними особами-підприємцями можна проілюструвати на практичних прикладах.

**Приклад 1.** Найманому працівникові нараховано заробітну плату за місяць 10000 грн. Із цієї заробітної плати роботодавець повинен відрахувати до бюджету податок на доходи фізичних осіб 18 % (1800 грн) та військовий збір 1,5 % (150 грн), а також додатково на нараховану заробітну плату сплатити 22 % – єдиний соціальний внесок (2200 грн). В підсумку фонд оплати праці такого працівника становитиме 12 200 грн, з чого працівник отримує на руки 8050 грн, а загальна сума податків та зборів складе 4150 грн.

**Приклад 2.** Фізична особа-підприємець, який є платником єдиного податку 3-ї групи згідно з цивільно-правовим договором отримав від юридичної особи (ІТ-компанії) плату за надані послуги в лютому 2019 р. у розмірі 10000 грн. ФОП має при цьому сплатити такі обов'язкові платежі: єдиний податок - 5 % від доходу (тобто 500 грн) та єдиний соціальний внесок – 22% від мінімальної заробітної плати (у 2019 році розмір ЄСВ становить 918 грн, у 2020 – 1039 грн). При цьому компанія-замовник послуг більше нічого додатково не нараховує та не стягує.

Очевидно, що друга модель співпраці є більш вигідною для ІТ-компаній. При цьому по суті «життєво» необхідною така модель є для стартапів – новостворених компаній (можливо, ще не зареєстрованих офіційно, але які всерйоз планують стати офіційними), що будують свій бізнес на основі інновацій та інноваційних технологій, але ще не вийшли на

ринок або тільки почали на нього виходити, маючи обмежені ресурси<sup>12</sup>. Для стартапів критичною є відсутність стабільного фінансування та капіталу, достатнього для забезпечення стабільних виплат працівникам, а, отже, й неможливість наймати їх взагалі на початкових етапах свого функціонування. Відтак для ІТ-компаній (особливо новостворених) надзвичайно важливим є можливість використання у своїй діяльності договорів із ФОП.

Укладення цивільно-правових договорів є також актуальним у контексті навчання та стажування молодосвідчених чи починаючих ІТ-спеціалістів. При цьому не слід плутати стажування з випробувальним терміном. Так, чинне законодавство про працю передбачає поняття випробувального терміну для новоприйнятих працівників. Однак випробувальний термін можна призначати не всім, адже закон передбачає перелік обмежень щодо окремих категорій працівників. Окрім того у разі, якщо працівник ще навчається відповідним навикам, то за три місяці (граничний строк випробування за законодавством) важко одночасно і навчити, і перевірити його здатність виконувати відповідну роботу. У такому разі укладення цивільно-правового договору, строк якого може й перевищувати три місяці, міг би бути виходом із ситуації. До того ж в плані оподаткування

Однак чинне законодавство передбачає стажування тільки для студентів (ст. 29 ЗУ «Про зайнятість населення»). Порядок стажування встановлений постановою КМУ від 16 січня 2013 р. № 20 «Про затвердження Порядку укладення договору про стажування студентів вищих та учнів професійно-технічних навчальних закладів на підприємствах, в установах та організаціях і Типової форми договору про стажування студентів вищих та учнів професійно-технічних навчальних закладів на підприємствах, в установах та організаціях». Натомість для тих, хто уже давно закінчив університет і має намір самостійно (в рамках самоосвіти) перекваліфікуватися, законодавство (зокрема КЗпП та Закон «Про зайнятість населення») такої можливості не передбачає. В сучасних умовах, коли формальна освіта уже давно не є ключовим орієнтиром для подальшого вибору професії, такий стан законодавства не лише не сприяє розвитку економіки, але й ускладнює його, створюючи додаткові перешкоди для людей, які вирішили знайти себе у іншій професійній сфері та стати більш корисним і більш високооплачуваним спеціалістом.

З точки зору принципу верховенства права застосування моделі співпраці з ІТ-спеціалістами за цивільно-правовими договорами не може автоматично вважатися порушенням та умисним приховуванням трудових відносин. Конституція України рівною мірою гарантує кожному громадянину, як право на підприємницьку діяльність, яка не заборонена законом (стаття 42), так і право на працю, що включає можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується (стаття 43). І ці два права аж ніяк не є взаємовиключними. Однак поняття "оптимізація податкових платежів" та "ефективне податкове планування" контролюючі органи досить часто вважають синонімічними до понять "умисне ухилення від сплати податків". Тому співпраця із ФОП – це досить актуальне та «болюче» на цей час питання для представників ІТ-галузі.

У разі якщо Держпраці за не врегульованими досі критеріями вирішить прирівняти такі відносини до замаскованих трудових, то крім захмарних штрафів за КЗпП (30 мінімальних заробітних плат) українським компаніям також загрожує проведення перевірки податковими органами, донарахування податкових зобов'язань та, ймовірно, навіть відкриття

---

<sup>12</sup> Бачинський, Т.В., 2017. Стартап в Україні: погляд з позиції ІТ-права. Т.В.Бачинський (Ред.), *Основи ІТ-права в Україні*, Київ, Юрінком Інтер, с.123-132

кримінального провадження за ст.212 КК. Залежно від «креативності» слідчого існує й загроза відкриття кримінального провадження за ст. 209 КК проти керівництва компанії, що, у свою чергу, створює загрозу застосування заходів кримінально-правового характеру до самої ІТ-компанії. Звісно, довести до суду таку «роздуту» справу майже не вбачається реальним. До того ж наразі відсутня практика застосування заходів кримінально-правового характеру до юридичних осіб, адже цей правовий інститут з моменту самої ж появи у КК України, викликав більше питань, ніж відповідей. Однак у арсеналі недобросовісного слідчого завжди зберігається можливість дестабілізувати роботу підприємства у такий спосіб, особливо якщо йдеться про рейдерські схеми та схеми недобросовісної конкуренції з участю в них правоохоронних органів.

Наразі ж судова практика частіше стає на бік роботодавців, а не контролюючих органів, які переважно керуються чисто фіскальною, а не правовою позицією. Запорукою успішного захисту від необґрунтованих претензій державних органів насамперед є доведення того, що мали місце саме господарські відносини з незалежним суб'єктом господарювання (наприклад, підрядником чи надавачем послуг) у рамках провадження звичайної господарської діяльності. Трудові відносини при цьому юридично відсутні, оскільки немає факту укладення трудового договору.

Фактичних критеріїв або конкретних підстав для розмежування господарських чи цивільно-трудових і трудових відносин чинне законодавство не містить. Однак судова практика робить наступні висновки щодо ознак, які відрізняють цивільні відносини від трудових: 1) трудовим законодавством врегульовано процес організації трудової діяльності, натомість за цивільно-правовим договором процес організації трудової діяльності залишається за його межами, а метою договору є отримання певного матеріального результату; 2) виконавець, який працює за цивільно-правовим договором, на відміну від працівника, який виконує роботу відповідно до трудового договору, не підпорядковується правилам внутрішнього трудового розпорядку, хоча й може бути з ними ознайомлений, і сам організовує свою роботу та виконує її на власний ризик; 3) виконавця за цивільно-правовим договором не зараховують до штату установи (організації), не вносять запису до трудової книжки та не видають розпорядчий документ про прийом його на роботу на певну посаду (див. постанову П'ятого апеляційного адміністративного суду від 30.10.2019 р. у справі № 400/206/19). Керуючись такими критеріями під час укладення цивільно-правового договору (насамперед важливо звертати увагу на термінологію договору, яка не має перегукватися із положеннями трудового законодавства), є всі підстави у судовому порядку захиститися від необґрунтованих звинувачень контролюючих органів.

На початку 2019 року Мінсоцполітики України презентувало для обговорення законопроект з нібито благородною метою та не менш промовистою назвою - **щодо посилення захисту прав працівників та протидії застосуванню незадекларованої праці**<sup>13</sup>. Згодом відповідний проект закону був зареєстрований у Верховній Раді, чим викликав хвилю критики, особливо у ІТ-середовищі. Вкрай саркастичні, однак змістовні зауваження виклала Оксана Кочкодан, долевий юрист Axon Partners:

---

<sup>13</sup> Проект Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав працівників та протидії застосуванню незадекларованої праці», 2019. Міністерство праці та соціальної політики України. [online] Документ доступний за посиланням: <https://www.msp.gov.ua/projects/401/>



*«Термінологія з Цивільного кодексу України кочує в Кодекс законів про працю України. Законодавчий акт 1971 року стає ще більш стильним і молодіжним. Ти думаєш, що надаєш послуги за цивільно-правовим договором? Куди там, твій замовник – твій роботодавець. А, отже, те, що між вами відбувається, – «трудові відносини». Принаймні, якщо містить одну з трьох ознак, не потрапити під яку можна тільки випивши святої води на Водохреще: 1) тобі періодично платять за послуги; 2) ти нікому не передаєш свої завдання, бо над тобою є наглядач, який все бачить і командує; 3) 75% доходу і більше протягом 6 місяців – тільки за цю роботу; 4) в тебе є робоче місце і правила, як там поводитися; 5) крім тебе, в роботодавця ще десяток таких, як ти, які роблять те саме, але за трудовим договором; 6) комп'ютер і блокнот з ручкою тобі дав роботодавець; 7) ти працюєш і відпочиваєш у чітко визначений роботодавцем час»<sup>14</sup>.*

У серпні 2019 року новообраний парламент відкликав цей законопроект, однак питання критеріїв прирівнювання цивільно-правових відносин до трудових залишилося не знятим. З вуст прем'єр-міністра та урядовців пролунали пропозиції ввести окрему 5-у групу спрощеної системи оподаткування для ІТ-індустрії та запровадити для неї спеціальні умови оподаткування. Пропонується, що крім звичних 5% єдиного податку, ФОП на 5-ій групі повинні будуть платити 1,5% військового збору, єдиний соціальний внесок з двох мінімальних заробітних плат, а також так званий збір на розвиток людського капіталу – 1% від доходу, починаючи з 2020 року, з поступовим підвищенням його до 5% до 2024 року (має сплачуватися до спеціального недержавного фонду, який незрозумілим чином повинен адмініструватися представниками ІТ-галузі). Тим самим ІТ-підприємців планують вивести з групи ризику визнання цивільно-правових відносин *де-факто* трудовими. При цьому, перехід на нову групу оподаткування для ФОП ІТ-індустрії буде добровільним, бажаючи зможуть і далі працювати на 3-ій групі єдиного податку<sup>15</sup>.

З точки зору стабільності ведення бізнесу, пропозиція, можливо, й слухна (однак все залежить від того, як її будуть реалізовувати на практиці), а от з точки зору принципу верховенства права – так само вкрай дискусійна з огляду на абсурдність протиставлення права на працю та права на підприємницьку діяльність. Адже на практиці це може створити наступну ситуацію: 1) якщо ви програміст, що зареєстрований ФОПом на спрощеній системі оподаткування (3 група), то ваші відносини із замовником можуть прирівняти до трудових; 2) якщо ж ви перейдете на іншу, спеціальну групу оподаткування для ІТ-спеціалістів і будете платити інші внески (при цьому не лише у держбюджет, а й у згаданий вище недержавний Фонд розвитку людського капіталу – так званий ІТ Creative), то тоді у податкових органів та інспекції Держпраці питань нібито не буде виникати (чому – невідомо, мабуть тому, що просто так «креативно» і «по-сучасному» вирішили в уряді, а на Конституцію та законодавство звертати увагу не обов'язково...). Критерії ж визнання цивільно-правових відносин так само залишаються невизначеними та незрозумілими з точки зору Конституції України та поваги до прав людини. Цілком можливо, що такі пропозиції також будуть відкинуті з позиції їх невідповідності принципам правової держави. Однак привертає увагу

<sup>14</sup> Ярова, М., 2019. Нова загроза для ФОПів в ІТ: що пропонує Мінсоцполітики в новому законопроекті. *AiN*. [online] Режим доступу: <https://ain.ua/2019/02/14/nova-zagroza-dlya-fopiv-v-it/>

<sup>15</sup> Мінфін, 2019. Що влада пропонує ІТ-індустрії. [online] Режим доступу: <https://minfin.com.ua/ua/2019/09/06/38970511/>

сам факт нехтування елементарними засадами функціонування демократичного суспільства під час формування економічної політики держави.

На наш погляд, важливо насамперед не створювати міфів про те, що вітчизняний ІТ-сектор нібито використовує недобросовісні схеми, які завдають збитків державному бюджету (адже в цьому й весь корінь згаданих «новацій» та пропозицій). Вказаний міф було спростовано у **Аналітичному звіті «Розвиток української ІТ-індустрії»**, підготовленого та опублікованого в жовтні 2018 року за ініціативи Асоціації «ІТ Україна» спільно з Офісом ефективного регулювання (BRDO). У документі, зокрема, вказано наступну важливу інформацію, з якою цілком погоджується Державна регуляторна служба України<sup>16</sup>, критикуючи пропозиції Мінсоцполітики:

*«Специфіка ринку ІТ в тому, що лівова частка витрат (більше 80%) становить оплата праці. У промисловості цей показник в межах від 8% до 15%. Тому, податки на заробітну плату в ІТ фактично є податками із обороту. Перевагою ІТ сфери, де близько 80% відсотків витрат це заробітна плата, є те, що ці кошти отримують фізичні особи, які витрачають їх в Україні, напряду стимулюючи внутрішній ринок. Крім того, дохід співробітників, що перебували у трудових відносинах з компаніями, перевищував середню зарплату в 7 разів, а дохід ФОП — у 7.8 раза. Таке співвідношення зберігається протягом тривалого часу.*

*Відповідно і розмір надходжень до державного бюджету на одного працюючого в сфері ІТ був значно вищий, ніж в середньому по країні. Податок на доходи фізичних осіб, сплачений працівниками ІТ-галузі, у 3.7 раз перевищував середній по країні. Оскільки у галузі широко застосовують модель співпраці зі спеціалістами на умовах ФОП, враховувався також розмір єдиного податку, сплачений одним активним підприємцем. Тим не менш, його розмір виявився також у 3.4 рази більшим, ніж розмір ПДФО на 1 працюючого. При цьому обсяг надходжень до бюджету від цього податку в ІТ-секторі зростав у середньому на 58,8% протягом 2013–2017 років і становив 3,2 млрд грн у 2017.*

*Слід також зазначити, що єдиний податок, який сплачують ФОП, на 100% залишається в місцевих бюджетах за місцем реєстрації, тоді як ПДФО розподіляють серед місцевих бюджетів різного рівня на 75%, а податок на прибуток на 90% надходить до центрального. Тож можна сказати, що працівники ІТ-сфери сприяють наповненню місцевих бюджетів і розвитку регіонів»<sup>17</sup>.*

---

<sup>16</sup> Державна регуляторна служба України, 2019. ДРС категорично проти ініціатив Мінсоцполітики щодо ФОП, зважаючи на ризики для економіки України. [online] Режим доступу: <http://www.drs.gov.ua/press-room/drs-kategorichno-proty-initsiatyv-minsotspolityky-shhodo-fop-zvazhayuchy-na-ryzyky-dlya-ekonomiky-ukrayiny/>

<sup>17</sup> Асоціація «ІТ Україна» та Офіс ефективного регулювання (BRDO), 2018. Розвиток української ІТ-індустрії. Аналітичний звіт, Київ. [online] Режим доступу: [https://ko.com.ua/files/u125/Ukrainian\\_IT\\_Industry\\_Report\\_UKR.pdf](https://ko.com.ua/files/u125/Ukrainian_IT_Industry_Report_UKR.pdf)

### 4.3. Юридичний супровід ІТ-бізнесу в умовах глобалізації економіки

У практиці вітчизняних ІТ-відносин гостро відчуються як наявність прогалин у праві, так і брак сучасного правового регулювання. Це призводить до того, що ІТ-право існує не лише в тих відносинах, які не врегульовані нормами закону, а й часто всупереч їм. У зв'язку із цим виникає необхідність застосування аналогії в праві та звертання до актів міжнародно-правового характеру, а також впровадження комплаєнс-практик на основі положень зарубіжних нормативно-правових актів (зокрема, законодавства США та ЄС).

Відтак специфіка ІТ-права полягає у тому, що це ще й право без кордонів і сучасному ІТ-юристу недостатньо володіти лише знаннями національного законодавства. Вкрай необхідно орієнтуватися у особливостях міжнародно-правового регулювання відносин у цифровому середовищі, а також розуміти особливості зарубіжної практики юридичного супроводу ІТ-бізнесу.

Так, нерідко перед ІТ-бізнесом постає питання вибору оптимальної юрисдикції. І питання не лише в податковому структуруванні (і не в офшорних схемах, хоча й це не виключено, якщо йдеться про недобросовісне підприємництво), а й у захищеності інтелектуальної власності та захисті бізнесу в цілому (наприклад, від рейдерства). Окрім того ІТ-контракти у сфері ЗЕД теж вимагають обізнаності зі специфікою законодавства та судової практики сторони-замовника (із цим може бути пов'язаний вибір застосовного права за договором). На жаль, іноземні замовники ІТ-послуг вкрай рідко погоджуються включати в контракт норми про застосовне право України та вирішення усіх спорів в українських судах. І на це є об'єктивні причини... Тому уже звичною справою є норми договорів про застосовне право, наприклад, одного зі штатів США, Республіки Ірландія тощо. Відтак ІТ-право найшвидше відчуває на собі усі «віяння» західних правових систем і не тільки.

#### **Приклад щодо застосовного права**

*Український програміст є співзасновником ІТ-компанії, що зареєстрована в Естонії (у цій країні більш лояльне податкове законодавство, зокрема, запроваджений податок на виведений капітал). З'явилися замовники з Бельгії, укладено контракт на створення програмного забезпечення. При цьому у контракті застосовним правом вказано право Штату Делавер (США). Причини можуть бути різні: а) у бельгійців там є своє постійне представництво і основна діяльність здійснюється в Делавері; б) в цьому штаті заходяться сервери з онлайн-платформою, на якій будуть створювати програмне забезпечення; в) інший варіант. Кошти за контрактом будуть надходити на рахунок естонської компанії. В такій ситуації може виникнути одразу кілька питань:*

- *яким чином отримати свою винагороду кінцевому бенефіціару (українському програмісту), щоб не витратити більшу суму на податки (можливі варіанти: дивіденди, заробітна плата, винагорода за іншим договором субпідряду тощо);*
- *де будуть розглядатися можливі спори за контрактом;*
- *як в Україні/Естонії виконати рішення іноземного суду та інші питання.*

Додатково можна навести приклад із практики, коли у контракті із компанією-замовником зі США застосовне право визначалося залежно від регіону світу, в який постачалися програмні послуги. Якщо це США, то застосовним вважалося право штату Каліфорнія, для країн економічного регіону EMEA (Європа, Близький Схід, Африка) – право Республіки Ірландія, для країн Азії – право Сінгапуру і т.д. На практиці механізм визначення застосовного права у таких ситуаціях виглядає наступним чином:

- контракт на послуги є рамковим, усі деталі містяться в додатках до нього, один із яких SoW (Statement of Work або аналог додаткової угоди з технічним завданням, цінами, строками тощо);
- у кожному конкретному SoW вказується, куди саме (в яку країну) постачаються послуги програмування;
- залежно від того, чого саме стосується спір (якого конкретно SoW), визначається регіон, в який постачалася послуга, та здійснюється вибір застосовного права і судового органу відповідно до казуальних норм контракту.

Окрім того, виникає чимало ситуацій, коли правові відносини у IT-сфері взагалі не врегульовані правом України. Зокрема питання щодо законності з точки зору українського права мають:

- договори про нерозголошення (**NDA** або **Non-Disclosure Agreement**);
- положення договорів про непереманювання (**buyout clause**);
- договори про неконкуренцію (**NCA** або **Non-Compete Agreement**);
- договори про обробку даних (**DPA** або **Data Processing Agreement**).

Питання щодо правової природи цих договорів, їх ефективності та доцільності укладення є дискусійними та активно обговорюються у фаховій літературі та під час тематичних конференцій, семінарів та вебінарів. Однак, незважаючи на це, вказаними аббревіатурами пересічного айтишника уже важко здивувати. Більше того, в українських IT-компаніях уже давно й активно укладають такі договори (або передбачають норми відповідного змісту у основних контрактах), а більшість програмістів їх дотримуються. Водночас положення цих документів більшою чи меншою мірою вступають в суперечність із економічними правами та свободами (зокрема, правом на працю та правом на свободу підприємницької діяльності). При цьому не слід помилково вважати, що це проблема виключно вітчизняної правової системи та її «відсталості» у відповідних аспектах від більш «прогресивних» зарубіжних правових систем. Насправді, навіть у багатьох штатах США суди негативно ставляться до положень договорів про неконкуренцію (NCA) та про непереманювання (buyout clause), визнаючи їх такими, що непропорційно обмежують економічні права і свободи громадян. Однак про все по-порядку.

**Угоди за типом NDA** є звичною практикою в питаннях взаємодії між іноземними замовниками (насамперед зі США) та українськими виконавцями IT-послуг. Найчастіше у цих договорах дається вказівка на застосовне право – право того чи іншого штату США. Цей пункт часто викликає саркастичну посмішку в українських юристів. Однак питання можливого недотримання зобов'язань за договорами NDA лежить зовсім не у площині судових спорів за американським правом та проблемах механізму виконання рішень судів США в Україні<sup>18</sup>. Є

---

<sup>18</sup> Бачинський, Т.В., 2017. Конфіденційність та способи захисту комерційної таємниці. NDA (договір про нерозголошення). Т.В. Бачинський (Ред.), *Основи IT-права*, Київ, Юрінком Інтер, с.141-150

інший, більш дієвий запобіжник від недобросовісної підприємницької практики з боку українських айтишників – ризик визнання відповідного суб'єкта господарювання недобросовісним партнером, якому доступ до ринків ІТ-послуг США та ЄС у зв'язку із цим може бути закритий. До того ж, норми українського законодавства містять достатньо положень про захист комерційної таємниці (статті 117, 420, статті 505-508 глави 46, статті 862, 1116 Цивільного кодексу; статті 25, 32, 36, 155, 162 Господарського кодексу, стаття 232 Кримінального кодексу). Посилаючись на них, ІТ-юристи обґрунтовують можливість функціонування у вітчизняній правовій системі таких видів договорів як NDA.

Також слід врахувати те, що ІТ-компанії в Україні створюються переважно у формі ТОВ. А тому важливими є й норми Закону «Про товариства з обмеженою відповідальністю та товариства з додатковою відповідальністю» щодо захисту комерційної таємниці. Так, статтею 42 Закону передбачена пряма заборона для посадових осіб товариства розголошувати інформацію, що стала їм відома у зв'язку з виконанням ними посадових обов'язків та становить комерційну таємницю товариства чи є конфіденційною, крім випадків, коли розкриття такої інформації вимагається законом. Крім того, що за законом порушення таких обов'язків є підставою для розірвання товариством договору (контракту) з посадовою особою без виплати компенсації, це також є підставою для притягнення до кримінальної відповідальності за статтею 232 КК. Передбачається, що таким чином Закон про ТОВ та ТДВ з часом може «розморозити» цю статтю 232 КК, за якою в судовому реєстрі наразі не вдається знайти жодного вироку.

**Пункти про непереманювання (buyout, а також buyout clause або release clause)** – це такі положення договору, що надають право замовнику самостійно напряму працювати з співробітниками або підрядниками виконавця виключно за умови, що замовник виплатить встановлену винагороду на користь виконавця<sup>19</sup>.

Пункт про buyout може бути сформульованим у контракті таким чином:

... if the Company wishes to establish the contractual relations with the developer involved by the Contractor, the Contractor must agree to the arrangement in writing, and the Company must pay ...	... Якщо Компанія (замовник) бажає встановити договірні відносини із розробником, залученим Виконавцем, Виконавець повинен письмово погодитись на таку угоду, а Компанія (замовник) повинен сплатити...
---	---

Окрім того практикуючи ІТ-юристи стверджують, що release clause в Україні можливо юридично коректно описати в рамках пункту про збереження конфіденційної інформації. У такому разі робота замовника напряму із підрядником буде вважатися неналежним використанням конфіденційної інформації компанії, за що може стягуватися штраф. Хоч запропонований варіант не є панацеєю і не гарантує 100% успіху у разі виникнення відповідного спору, але він успішно використовується в превентивних цілях, щоб мінімізувати можливі ризики шахрайської поведінки замовника<sup>20</sup>.

Слід відзначити, що положення про непереманювання можуть передбачатися не лише у контрактах між компанією-замовником та компанією-виконавцем ІТ-послуг, але й

<sup>19</sup> Голод, О., 2019. Buyout clause: як утримати ІТ спеціаліста. *Lagal IT Group*. URL: <https://legalitygroup.com/buy-out-in-it/?fbclid=IwAR1yXc0J5nqnrX61yKXZqgGeB7VBVZvZmt3ZcrkvSt1yO6pSgbG5h1621qU>

<sup>20</sup> Голод О. Згадана публікація.

між компанією-виконавцем та її працівниками чи підрядниками. Останнє, зокрема, стосується уникнення ситуацій, коли звільняється один кваліфікований співробітник, створює власну компанію і переманює до себе цілу команду своїх колег. Суттєвий відтік кадрів протягом обмеженого проміжку часу може призвести до тимчасової виробничої неспроможності ІТ-компанії та, як наслідок, до зриву виконання контрактів із замовниками. Також виникають додаткові витрати, пов'язані із пошуком та навчанням нових працівників на заміну тим, що звільнилися. Тому в контексті запобігання недобросовісній конкуренції відповідні умови про buyout у контрактах зі співробітниками ІТ-компанії виглядають цілком виправданими та обґрунтованими. У конструкцію цивільно-правових договорів з ФОПами-підрядниками, на нашу думку, такі умови можна включати без вагань. Водночас відповідні умови трудових договорів, ймовірно, можуть бути визнані «неприпустимими» з точки зору контролюючих органів (зокрема інспекторів Державної служби з питань праці), які досі звикли керуватися виключно заформалізованими положеннями постсоціалістичного трудового законодавства України. Однак, на наш погляд, незважаючи на відсутність сформованої судової практики у питаннях застосування buyout в Україні, не варто боятися передбачати такі зобов'язання і для працівників. Важливо розглядати ситуацію з позиції права на захист від недобросовісної конкуренції.

Перш за все слід керуватися тим, що принцип недопущення недобросовісної конкуренції в Україні передбачений на конституційному рівні (абзац другий статті 42 Конституції України). Цим же положенням закріплено обов'язок держави (в особі уповноважених органів) забезпечувати захист конкуренції у підприємницькій діяльності. Відповідні конституційні положення були конкретизовані у статті 13 Цивільного кодексу, главі 3 Господарського кодексу та у нормах спеціальних законодавчих актів (ЗУ «Про захист економічної конкуренції», ЗУ «Про Антимонопольний комітет»). З огляду на це, release clause для працівників більш доцільно передбачати у окремих угодах цивільно-правового характеру та захищати такі положення документу умовами про конфіденційність. У разі порушення працівником зобов'язання відповідний спір може бути переданий на розгляд суду в рамках цивільного чи господарського судочинства (залежно від предмету спору та конкретних обставин справи). При цьому не виключаємо й участь Антимонопольного комітету у врегулюванні ситуацій, коли недобросовісна діяльність колишнього співробітника ІТ-компанії має ознаки антиконкурентних узгоджених дій у змові з іншими компаніями-конкурентами колишнього роботодавця.

**Договір про неконкуренцію (NCA)** є своєрідним дзеркальним відображенням buyout clause. Зокрема, це договір, який укладається між роботодавцем і працівником, який обмежує останнього від роботи в будь-якому подібному бізнесі впродовж роботи у роботодавця та протягом певного періоду часу після припинення трудових відносин. В зарубіжній практиці зобов'язання по NCA найчастіше включаються в загальний трудовий договір. Однак в Україні таке положення трудового договору буде прямо суперечити статті 9 КЗпП, відповідно до якої умови договорів про працю, які погіршують становище працівників порівняно з законодавством України про працю, є недійсними. Більш того, судова практика в Україні, свідчить про визнання незаконними будь-яких положень договорів, які обмежують право особи займатися тією чи іншою діяльністю (незалежно від обмеження певними видами або терміном).

З іншого боку, відповідно до статті 21 КЗпП працівник має право реалізувати свої здібності до продуктивної і творчої праці шляхом укладення трудового договору на одному

або одночасно на декількох підприємствах, в установах, організаціях, якщо інше не передбачене законодавством, колективним договором або угодою сторін. Тож, зважаючи на згадку про угоду сторін, виглядає виправданим укладати самостійні договори про неконкуренцію (або передбачати відповідні положення у договорах NDA) хоча б на період трудових відносин між працівником та роботодавцем. У обох випадках NCA-зобов'язання варто обґрунтовувати з точки зору необхідності збереження конфіденційності між сторонами (робота на компанію-конкурента напряду суперечить цьому принципу). Це, зокрема, виступить стримуючим фактором для ІТ-спеціалістів, які можуть спробувати одночасно працювати на декілька компаній.

**Приклад «розумних» умов NCA в ІТ-контракті:**

<p><i>Outside work (whether paid or unpaid) may only be permitted if it is limited in scope, does not interfere with your work at ... , and does not utilize company's resources. Performing work for an ... competitor is not allowed under any circumstances</i></p>	<p><i>Робота на стороні (незалежно оплатна вона чи ні) може бути дозволена, лише якщо вона обмежена за обсягом, що не заважає вашій роботі з ... та не використовує ресурси компанії. Виконання робіт для конкурента ... не допускається ні за яких обставин.</i></p>
--	---

З цього положення випливає наступне:

- інша оплачувана робота не забороняється, однак вона може здійснюватися у час, відмінний від основної роботи та без використання ресурсів основного роботодавця.
- виконання робіт для конкурента є неприпустимим та означає виконання робіт як за трудовим, так і за цивільно-правовим договором (зокрема й у статусі ФОП).

В будь-якому разі, укладаючи договори NCA важливо звертатися до зарубіжної практики, особливо якщо йдеться про контракт з іноземним замовником із вказівкою на застосовне право іншої країни.

Так, у більшості штатів США, де положення NCA узаконені, існують такі вимоги до цього документу: 1) добровільність сторін при укладанні; 2) розумне територіальне обмеження; 3) тимчасові рамки дії (6 місяців - 3 роки); 4) сфера діяльності або галузь; 5) санкції за порушення (працівника можуть звільнити, позбавити пільг, додаткових виплат або вихідної допомоги, колишній роботодавець може подати в суд, якщо співробітник відмовляється підписувати NCA при звільненні). У Великобританії з середини 19-го століття застосовуються умови про тимчасове обмеження будь-якої професійної діяльності працівника (garden leave): протягом певного періоду часу (до 12 місяців) працівник продовжує отримувати заробітну плату в колишньому розмірі, але позбавляється доступу до комерційної інформації роботодавця і права займати аналогічну позицію чи інакше конкурувати після звільнення. Роботодавець щомісячно виплачує працівникові не менше 1/3 середнього заробітку за останній рік. Термін дії варіюється від 6 місяців до 3-х років. За компенсації - можуть відрізнятись розміри і механізми формування. Сторони можуть домовитися про одноразову компенсацію, збереженні повної заробітної плати на час garden leave / її половини. У таких країнах, як Франція, Німеччина, Італія, Голландія та Іспанія, NCA

має передбачати істотну компенсацію для співробітника. Причому чим більший термін дії застереження і чим воно жорсткіше, тим більшою повинна бути компенсація<sup>21</sup>.

Укладення **договорів про обробку даних** за типом **DPA** в Україні є порівняно новою практикою, яка раніше не була поширеною. Зростання популярності таких документів пов'язане із набуттям чинності в ЄС у травні 2018 року Загального регламенту захисту даних (GDPR). Угоди за типом DPA можуть укладатися як самостійний документ або як додаток до основного контракту, який стосується надання ІТ-послуг, пов'язаних з обробкою даних, та передбачають положення про:

- види та перелік інформації, що підлягає обробці компанією-виконавцем від імені компанії-замовника;
- порядок обробки інформації;
- технічні та організаційні заходи захисту інформації (відповідно до ст.32 GDPR);
- порядок повідомлення про витік інформації чи інші порушення, пов'язані із обробкою даних

Певною мірою такі угоди «вписуються» у положення вітчизняного законодавства про інформацію (ЗУ «Про інформацію», ЗУ «Про захист персональних даних» тощо). Хоча, ймовірно, з продовженням євроінтеграційних процесів та зближенням української правової системи з правом ЄС, в положення вітчизняного законодавства будуть імплементовані відповідні норми GDPR.

Слід зауважити, що окрім необхідності володіти знаннями міжнародного права, а також специфіки зарубіжних правових систем, для ІТ-юриста важливо також оволодіти управлінськими навиками. Так, у сучасному світі юристу недостатньо бути просто хорошим фахівцем у своїй справі. Успішний юрист повинен бути ще й хорошим менеджером (незалежно від того, працює він у бізнесі чи у державному секторі). Відповідні навички впливають на ефективне вирішення юридичних завдань у їх системному взаємозв'язку із завданнями інших підрозділів підприємства, установи чи організації. Так, фахівці з менеджменту висувують нові вимоги до підготовки юристів у вищій школі: «майбутні юристи повинні мати не тільки глибокі управлінські знання, а й сформувати вміння та навички юридичного управління організаціями на різних рівнях та посадах ... потрібно відчувати можливості й наслідки впливу права на економіку та управління<sup>22</sup>.

Тісний взаємозв'язок бізнес-процесів та юридичної практики простежується саме у ІТ-сфері, де юристу важливо:

- а) розуміти загальну специфіку (включаючи технічну складову) надання відповідних послуг ІТ-компанії;
- б) брати участь у підготовці бізнес-пропозицій;
- в) вміти вибудувати правильну лінію укладення та подальшого супроводу договорів, виходячи із «настроїв» замовника та можливостей компанії-виконавця відповідних послуг;
- г) володіти навиками налагодження внутрішніх бізнес-комунікацій у середовищі конкретних виконавців послуг (ІТ-спеціалістів).

---

<sup>21</sup> Чута, І., 2018. Как соглашение о неконкуренции (NCA) работает в Украине и в мире, *DigiLaw Ukraine*, [online] Режим доступа: <https://medium.com/digilaw-ukraine/как-соглашение-о-неконкуренции-nca-работает-в-украине-и-в-мире-с9с38706а906>

<sup>22</sup> Шевченко, Л.С., 2019. *Стратегічний бізнес-консалтинг*: навч. посіб. Харків, Право, с.281-282



Без таких знань та умінь юридичний супровід співпраці із замовником буде ізольованим від реальних бізнес-процесів, а тому він є не лише малоефективним, але й навіть може ускладнювати, гальмувати чи навіть погіршувати розвиток ІТ-компанії. За таких обставин менеджерські навички є однією із ключових складових професіоналізму ІТ-юриста.

#### 4.4. Економічна складова екстериторіальної юридичної відповідальності у ІТ-сфері

Враховуючи сучасні тенденції глобалізації економічних процесів, можна виділити три «кити» правового супроводу ІТ-бізнесу в Україні:

- 1) **Compliance** як культура доброчесності ведення бізнесу. Передбачає у собі аналіз відповідності поведінки компанії принципам добросовісної поведінки на ринку, вимогам нормативних актів (не лише вітчизняних, а й, насамперед, міжнародних чи зарубіжних)
- 2) **Due diligence** – встановлення достовірності фінансової, податкової та статистичної звітності, правильності оформлення всіх документів компанії, їх відповідності законодавству та внутрішнім вимогам.
- 3) **Forensic** – діяльність із виявлення ключових господарських ризиків, аналізу та врегулювання фінансово-правових спорів та інших конфліктних ситуацій, які виникають між діловими партнерами<sup>23</sup>.

Запровадження перелічених стандартів ведення бізнесу є актуальним для ІТ-компаній у контексті таких (уже частково згаданих вище) документів, як:

- 1) Федеральний Закон США про податкову звітність за зарубіжними рахунками (англ. Foreign Account Tax Compliance Act, **FATCA**, 2010),
- 2) Федеральний Закон США про корупцію за кордоном (англ. Foreign Corrupt Practices Act, **FCPA**; 1977)
- 3) Загальний регламент ЄС про захист даних (англ. General Data Protection Regulation, **GDPR**; Regulation (EU) 2016/679).

Перелічені документи мають екстериторіальну дію, у зв'язку із чим українські компанії зацікавлені імплементувати закладені у них стандарти у власній господарській практиці з тим, щоб:

- 1) в очах закордонних партнерів (клієнтів, замовників) відповідати образу надійного та добросовісного партнера, з яким можна мати справу;
- 2) не наразитися на штрафні чи репутаційні санкції, пов'язані із порушенням вимог цих документів.

Так, положення **FATCA** зобов'язують іноземні фінансові організації звітувати перед Службою внутрішніх доходів США про рух коштів американських платників податків. В протилежному разі фінансові організації ризикують отримати санкції у вигляді 30-відсоткових штрафів на рух коштів з їх кореспондентських рахунків в банках США або й навіть закриття таких рахунків. Сьогодні положення FATCA активно впроваджуються українськими банками, кінцевими бенефіціарами яких є закордонні суб'єкти. Все частіше при відкритті банківського рахунку українські компанії стикаються з необхідністю заповнити спеціальну форму FATCA.

<sup>23</sup> Шевченко, Л.С. Згадана праця, с.289-291

При чому це стосується не лише компаній, в яких є іноземні засновники. Зазвичай для того, щоб ідентифікувати клієнта, банк просить вказати в анкеті FATCA тип компанії, для якої відкривається рахунок. Такими типами можуть бути або фінансова або нефінансова компанія. Якщо це нефінансова компанія, то вона може бути активною або пасивною нефінансовою компанією. Залежно від типу компанії визначається і обсяг інформації, яку буде збирати банк. Наприклад, пасивна нефінансова компанія повинна надати також відомості про бенефіціарів свого бізнесу, щоб підтвердити, що там немає резидентів США. У свою чергу, вимоги до активної нефінансової компанії значно менші.

**FCPA** накладає заборону на надання, пропозицію або обіцянку надати будь-яку благо іноземному посадовцю, політику, державному службовцю або співробітнику державної установи з метою отримання неправомірних переваг. Фактично такою особою може бути будь-яка іноземна особа, яка пов'язана з державою, здійснює публічні функції і отримує зарплату з державного бюджету країни. Екстериторіальна дія FCPA означає, що, наприклад, українська компанія може опинитися під прицілом його норм, якщо вона:

- здійснює свою діяльність в США,
- її акції котируються на американській біржі,
- є представництвом або дочірнім підприємством американської компанії,
- діє від імені американської компанії,
- обслуговує клієнтів з США,
- здійснює розрахунки в доларах США,
- використовує email-сервери США<sup>24</sup>.

Суворі санкції FCPA не є чимось надто далеким та невідомим для українських компаній, особливо для тих, які функціонують у сфері великого IT-бізнесу. Так, дію антикорупційного законодавства США уже відчула на собі компанія VEON (до 2017 VimpelCom) – глобальний провайдер телекомунікаційних послуг, що базується у Амстердамі та до складу якого входить український оператор мобільного зв'язку ПрАТ «Київстар». Цінні папери компанії VEON котируються на фондових біржах США. У 2016 році стало відомо, що компанія регулярно у період з 2006 по 2012 роки давала хабарі узбецьким чиновникам з метою одержання можливості надання телекомунікаційних послуг на ринку зв'язку Узбекистану. Внаслідок цього та на підставі положень FCPA у 2016 році компанія була оштрафована на суму 795 млн доларів<sup>25</sup>. Ще через три роки, у 2019 на подібних корупційних схемах і знову в Узбекистані була викрита російська телекомунікаційна компанія МТС. Штраф був ще більшим – 850 млн доларів<sup>26</sup>. Обидві компанії при цьому увійшли до списку топ-10 компаній, які заплатили найбільші штрафи за порушення FCPA.

Аналізуючи застосовність **GDPR** до українських компаній, слід врахувати кілька важливих аспектів. Так, за загальним правилом відповідно до частини першої статті 3 GDPR регламент застосовується до обробки даних у контексті діяльності осідку контролера або обробника в ЄС, незалежно від того, відбувається власне обробка в межах ЄС чи ні. Це

---

<sup>24</sup> Кожакар, О. 2019. Как США борются с коррупцией в Украине, *Економічна правда*. [online] Режим доступу: <https://www.epravda.com.ua/columns/2019/03/5/645830/>

<sup>25</sup> US Department of Justice, 2016. VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than \$795 Million; United States Seeks \$850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme. [online] Available at: <https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million>

<sup>26</sup> Cassin, Richard L., 2019. With MTS in the new Top Ten, just one U.S. company remains. The FCPA blog. [online] Available at: <https://fcpublog.com/2019/03/11/with-mts-in-the-new-top-ten-just-one-us-company-remains/>

зокрема означає, що у разі наявності офіційно зареєстрованого офісу компанії безпосередньо на території ЄС, норми GDPR є застосовними по відношенню до неї (навіть якщо головний офіс знаходиться поза межами ЄС). Водночас відсутність офіційно зареєстрованого представництва, філії чи дочірнього підприємства компанії на території ЄС не означає, що GDPR до такої компанії не застосовується. Іноді наявність навіть одного представника чи агента на території ЄС може розглядатися як те, що в компанії є осідок на території ЄС.

Більше того, як наголошують експерти, для України насамперед важливою є частина друга статті 3 GDPR, яка передбачає екстратериторіальну дію регламенту. В ній ідеться про те, що регламент застосовується до обробки персональних даних контролером або обробником, який має осідок поза межами ЄС (наприклад, компанія з України), якщо обробка пов'язана з постачанням товарів чи наданням послуг на території ЄС або з моніторингом поведінки суб'єктів даних, якщо така поведінка має місце на території ЄС. Перший важливий момент — послуги й товари можуть надаватися й безкоштовно. Другий — не обов'язково постачати ці послуги й товари, для застосування норм GDPR достатньо й «комерційного наміру». Окрім того варто взяти до уваги такі аспекти:

- мова, якою доступний сайт. Якщо сайт доступний мовою однієї з країн — членів ЄС, це є ознакою того, що компанія постачає товари та послуги на території ЄС;
- домен, зареєстрований у зоні ЄС;
- пропозиція поставки товарів чи надання послуг на території ЄС;
- прийом оплати в євро;
- чи має місце моніторинг поведінки суб'єктів даних на території ЄС<sup>27</sup>.

При цьому місце обробки персональних даних юридичного значення не має, так само як і місце перебування суб'єктів даних чи їхнє громадянство. Наприклад, якщо турист із Німеччини звернеться по послуги до української компанії, яка працює лише на території України, то ця компанія не буде зобов'язана підпорядковуватися GDPR. Або інший приклад — компанія, яка зареєстрована на території ЄС й здійснює обробку даних українських користувачів у Китаї, має підпорядковуватися GDPR. Це зумовлено тим, що вона зареєстрована в ЄС.

Арсен Кулик, сертифікований спеціаліст із застосування GDPR, наводить перелік прикладів, **що не можна робити ІТ-компаніям під загрозою штрафів за цим регламентом:**

- 1) ніколи не видаляти персональні дані користувачів (наприклад, зберігати їх прямо в blockchain або ж не передбачати можливості видалити свій профіль);
- 2) вимагати від користувачів згоду на обробку персональних даних, без якої вони не зможуть користуватися вашим сервісом;
- 3) вимагати надання персональних даних, які не є необхідними для конкретного виду пропонованих послуг<sup>28</sup>.

---

<sup>27</sup> Гордієнко, Т., 2019. GDPR в Україні: хто підпадає під дію норм нового регламенту? *Детектор Медіа*. [online] Режим доступу: <https://detector.media/infospace/article/144571/2019-02-04-gdpr-v-ukraini-khto-pidpadae-pid-diyu-norm-novogo-reglamentu/>

<sup>28</sup> Кулик, А., 2019. GDPR та український бізнес. 10 непростих запитань. *Інформаційно-правова система ЛІГА:ЗАКОН*. [online] Режим доступу: [https://biz.ligazakon.net/ua/news/184577\\_gdpr-ta-ukrainskiy-bznes-10-neprostikh-zapitan](https://biz.ligazakon.net/ua/news/184577_gdpr-ta-ukrainskiy-bznes-10-neprostikh-zapitan)

Можливість накладення штрафу з ініціативи контролюючих органів ЄС через їхню перевантаженість є малоюмовірною для українських компаній. Тому, швидше за все, штраф можуть накласти у разі надходження конкретної скарги від фізичної особи.

GDPR був введений в дію 25 травня 2018 року. Тому практика його застосування ще напрацьовується. Однак уже є перші «жертви» цього регламенту з числа суб'єктів великого ІТ-бізнесу. Зокрема, як повідомляє видання *The Verge*, Національна комісія з питань регулювання інформаційних технологій та прав людини Франції (CNIL) оштрафувала інтернет-гіганта Google на 50 млн євро за порушення GDPR-зобов'язань. Причина полягає в тому, що користувачам «може бути складно знайти інформацію стосовно мети збору даних, термінів зберігання даних та яка інформація використовується для налаштування рекламних оголошень»<sup>29</sup>.

Іншим прикладом застосування GDPR по відношенню до ІТ-компанії є справа, що була ініційована контролюючим органом Великої Британії (ICO) стосовно канадської компанії *AggregateIQ*, яка займається цифровим маркетингом та розробкою програмного забезпечення. Штраф у розмірі 17 000 000 фунтів стерлінгів може бути застосований до цієї компанії через те, що її діяльність пов'язує з діяльністю компанії *Cambridge Analytica*. Зокрема, у 2016 році *AggregateIQ* використала персональні дані з Facebook, якими раніше заволоділа *Cambridge Analytica*, для розробки програмного забезпечення, з допомогою якого здійснювалася цільова реклама виборців у США під час президентської кампанії. Відповідне повідомлення з вимогою усунення порушень та надання інформації було направлено *AggregateIQ* і по його невиконанню, згаданий вище штраф буде застосований<sup>30</sup>.

Аналізуючи практику застосування штрафних санкцій європейськими органами за порушення GDPR, ІТ-юристи зауважують, що контролюючими органами накладаються штрафи різних розмірів, залежно від вчиненого правопорушення. При цьому штрафи у більших розмірах накладаються в тих випадках, коли порушення стосуються або великих об'ємів персональних даних, або чутливих персональних даних. Головне, на що потрібно звернути увагу це той факт, що до відповідальності можуть бути притягнуті як компанії з території Європейського Союзу, так і компанії, які зареєстровані поза межами ЄС, про що яскраво свідчить справа, яка стосується притягнення до відповідальності канадської компанії *AggregateIQ*<sup>31</sup>.

Вказане свідчить, що вітчизняним ІТ-компаніям слід звикати до стандартів відкритості та прозорості ведення бізнесу, відмовившись від будь-яких сумнівних схем (включаючи співпрацю із компаніями з сумнівною чи негативною репутацією). В інакшому випадку існує значний ризик бути позбавленими доступу до західних ринків ІТ-послуг. Зокрема сьогодні існує низка глобальних баз даних, які збирають інформацію про бізнес-суб'єктів, які виходять на міжнародні ринки. Однією з таких баз є DUNS-реєстр (з англ. *Data Universal Numbering System* – «Всесвітня система нумерування даних»), який був створений ще у 1963 році американською компанією *Dun & Bradstreet (D & B)*. Заявленою метою створення реєстру D було підтвердження ділової репутації суб'єктів підприємницької діяльності. Сьогодні код

---

<sup>29</sup> Porter, J., 2019. Google fined €50 million for GDPR violation in France. *The Verge*. [online] Available at: <https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil>

<sup>30</sup> Clark, Anna Mercado, 2019. Better Compliance Through One Year of GDPR Enforcement, *Lexology*. [online] Available at: <https://www.lexology.com/library/detail.aspx?g=7df2fcbd-cc6e-468b-bcfa-9119eaa9ad28>

<sup>31</sup> Богарада, С., 2019. З штрафи за GDPR та висновки для українських компаній, *Legal IT Group*, [online] Режим доступу: <https://legalitgroup.com/3-shtrafi-za-gdpr-ta-visnovki-dlya-ukrayinskih-kompanij/>

DUNS (9-значний ідентифікаційний номер, який надається кожній компанії, що потрапляє в базу D&B) використовується в роботі понад 50 світових, промислових і торгових організацій, включно з ООН, Федеральним урядом США та Європейською комісією. При внесенні компанії в реєстр, співробітники агентства перевіряють, що компанія дійсно існує, строк її існування, наявність компанії за заявленим адресою офісу, кількість співробітників і так далі. Реєстрація компанії в каталозі D & B є першим кроком на шляху до того, щоб отримати підтвердження благонадійності компанії від авторитетної міжнародної організації.

Враховуючи викладене слід додати, що ризик визнання компанії неблагонадійною пов'язаний не лише із можливим порушенням відповідних стандартів добросовісного ведення бізнесу під час співпраці із закордонними партнерами. Важливого значення має й бізнес-історія компанії в Україні. Негативного забарвлення репутації вітчизняної компанії може додати умисне приховування факту притягнення менеджерів, акціонерів, співвласників бізнесу до кримінальної чи адміністративної відповідальності за минулі правопорушення у сфері економіки чи корупційні правопорушення. Тому напрямок налагодження комплаєнс-стандартів відповідно до положень FATCA, FCPA, GDPR та інших нормативних актів міжнародно-правового характеру сьогодні є одним із ключових для юристів українських ІТ-компаній.

### Список джерел

1. Cassin, Richard L., 2019. With MTS in the new Top Ten, just one U.S. company remains. The FCPA blog. [online] Available at: <https://fcpablog.com/2019/03/11/with-mts-in-the-new-top-ten-just-one-us-company-remains/>
2. Clark, Anna Mercado, 2019. Better Compliance Through One Year of GDPR Enforcement, Lexology. [online] Available at: <https://www.lexology.com/library/detail.aspx?g=7df2fcbd-cc6e-468b-bcfa-9119eaa9ad28>
3. Information Technology Law, Guide to IT Law. HG.org Legal Resources. [online] Available at: <https://www.hg.org/information-technology-law.html#1>
4. Michalsons, 2018. What is IT law, ICT law or Cyber law? [online] Available at: <https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286>
5. Porter, J., 2019. Google fined €50 million for GDPR violation in France. *The Verge*. [online] Available at: <https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnll>
6. US Department of Justice, 2016. VimpelCom Limited and Unitel LLC Enter into Global Foreign Bribery Resolution of More Than \$795 Million; United States Seeks \$850 Million Forfeiture in Corrupt Proceeds of Bribery Scheme. [online] Available at: <https://www.justice.gov/opa/pr/vimpelcom-limited-and-unitel-llc-enter-global-foreign-bribery-resolution-more-795-million>
7. Wehmeier, Tom and the Atomico Team, 2018. State of European Tech Report. [online] Available at: <https://2018.stateofeuropeantech.com/chapter/europes-got-talent/article/people-power/>
8. Асоціація «ІТ Україна» та Офіс ефективного регулювання (BRDO), 2018. *Розвиток української ІТ-індустрії. Аналітичний звіт*, Київ. [online] Режим доступу: [https://ko.com.ua/files/u125/Ukrainian\\_IT\\_Industry\\_Report\\_UKR.pdf](https://ko.com.ua/files/u125/Ukrainian_IT_Industry_Report_UKR.pdf)

9. Бачинський, Т.В., 2017. Конфіденційність та способи захисту комерційної таємниці. NDA (договір про нерозголошення). Т.В. Бачинський (Ред.), *Основи ІТ-права*, Київ, Юрінком Інтер, с.141-150
10. Бачинський, Т.В., 2017. Стартап в Україні: погляд з позиції ІТ-права. Т.В.Бачинський (Ред.), *Основи ІТ-права в Україні*, Київ, Юрінком Інтер, с.123-132.
11. Богарада, С., 2019. 3 штрафи за GDPR та висновки для українських компаній, *Legal IT Group*, [online] Режим доступу: <https://legalitgroup.com/3-shtrafi-za-gdpr-ta-visnovki-dlya-ukrayinskih-kompanij/>
12. Винничук, Р.О., Склярук, Т.В., 2015. *Особливості розвитку ІТ-ринку в Україні: стан та тенденції*. Вісник Національного університету "Львівська політехніка", Логістика, № 833, С. 3-8. [online] Режим доступу: [http://nbuv.gov.ua/UJRN/VNULPL\\_2015\\_833\\_3](http://nbuv.gov.ua/UJRN/VNULPL_2015_833_3)
13. Голод, О., 2019. Buyout clause: як утримати ІТ спеціаліста. *Legal IT Group*. [online] Режим доступу: <https://legalitgroup.com/buy-out-in-it/?fbclid=IwAR1yXc0J5nqnrX61yKXZqQGeB7VBVZvZmt3ZcrkvSt1yO6pSgbG5h1621qU>
14. Гордієнко, Т., 2019. GDPR в Україні: хто підпадає під дію норм нового регламенту? *Детектор Медіа*. [online] Режим доступу: <https://detector.media/infospace/article/144571/2019-02-04-gdpr-v-ukraini-khto-pidpadae-pid-diyu-norm-novogo-reglamentu/>
15. Державна регуляторна служба України, 2019. *ДРС категорично проти ініціатив Мінсоцполітики щодо ФОП, зважаючи на ризики для економіки України*. [online] Режим доступу: <http://www.drs.gov.ua/press-room/drs-kategorychno-proty-initsiatyv-minsotspolityky-shhodo-fop-zvazhayuchy-na-ryzyky-dlya-ekonomiky-ukrayiny/>
16. Інформаційне агентство «Інтерфакс-Україна», 2018. ІТ-індустрія в 2018 р. сплатить близько 10 млрд грн податків, [online] Відновлено з: <https://ua.interfax.com.ua/news/economic/541529.html>
17. Кожакар, О. 2019. Как США борются с коррупцией в Украине, *Економічна правда*. [online] Режим доступу: <https://www.epravda.com.ua/columns/2019/03/5/645830/>
18. Кулик, А., 2019. GDPR та український бізнес. 10 непростих запитань. *Інформаційно-правова система ЛІГА:ЗАКОН*. [online] Режим доступу: [https://biz.ligazakon.net/ua/news/184577\\_gdpr-ta-ukrainskiy-bznes-10-neprostikh-zapitan](https://biz.ligazakon.net/ua/news/184577_gdpr-ta-ukrainskiy-bznes-10-neprostikh-zapitan)
19. Мінфін, 2019. Що влада пропонує ІТ-індустрії. [online] Режим доступу: <https://minfin.com.ua/ua/2019/09/06/38970511/>
20. Новицький, А.В. (2016). *Місце ІТ-права в загальній системі інформаційного права*. Збірник матеріалів науково-практичної конференції «ІТ право: проблеми і перспективи розвитку в Україні», Львів, НУ «Львівська політехніка», С.116.
21. Опендатабот, 2019. Чому законопроект про ФОП може нашкодити саме ІТ-бізнесу? [online] Відновлено з: <https://opendatabot.ua/blog/294-jesuis-fop>
22. Підгайна, Є., 2018. Пішли на прорив: український ІТ-ринок зростає швидше за світовий, *Mind*. [online] Відновлено з: <https://mind.ua/publications/20189963-pishli-na-proriv-ukrayinskij-it-rinok-zrostaе-shvidshe-za-svitovij>
23. Проект Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав працівників та протидії застосуванню незадекларованої праці», 2019. *Міністерство праці та соціальної політики України*. [online] Документ доступний за посиланням: <https://www.msp.gov.ua/projects/401/>

24. Харитонов, Є.О. (2016). Сутність ІТ-права (ІТ-право як концепт). *Збірник матеріалів науково-практичної конференції «ІТ право: проблеми і перспективи розвитку в Україні»*. Львів, НУ «Львівська політехніка», с.274.
25. Харитонов, Є.О., Харитонova О.І., 2017. Поняття ІТ-права, сфера його дії та структура. Т.В. Бачинський (Ред.), *Основи ІТ-права*, Київ, Юрінком Інтер, с.7-22.
26. Чута, И., 2018. Как соглашение о неконкуренции (NCA) работает в Украине и в мире, *DigiLaw Ukraine*. [online] Режим доступа: <https://medium.com/digilaw-ukraine/как-соглашение-о-неконкуренции-нса-работает-в-украине-и-в-мире-c9c38706a906>
27. Шевченко, Л.С., 2019. *Стратегічний бізнес-консалтинг*: навч. посіб. Харків, Право.
28. Яворська, О.С., 2017. *ІТ-право*, Львів, Вид-во «Левада».
29. Ярова, М., 2019. Нова загроза для ФОПів в ІТ: що пропонує Мінсоцполітики в новому законопроекті. *AiN*. [online] Режим доступа: <https://ain.ua/2019/02/14/nova-zagroza-dlya-fopiv-v-it/>
30. Яценко, Т., 2019. Особливості оформлення трудових відносин в ІТ-компаніях і стартапах: теорія та практика. *ЮРИСТ&ЗАКОН*, №41, 14 листопада.