Основний акцент робиться на переорієнтації з кризового управління на середньо- і довгострокові реформи, що сприяють росту і зайнятості при стійкості державних фінансів, включаючи реформу пенсійних систем. Була підтверджена рішучість держав-членів невідкладно забезпечити бюджетну стабілізацію (хоча і в "різношвидкісному" режимі), передусім шляхом обмеження державних витрат і підвищення потенціалу зростання як основи оздоровлення фінансової системи в перспективі.

До кінця 2011 р. ЄК повинна представити проект комплексних заходів щодо реформи фінансової системи ЄС, що гарантує її безпеку, надійність, велику транспарентність і відповідальність, з урахуванням поточних стрес-тестів, проведених органами банківського нагляду. У зв'язку з цим Єврорада призвала Раду ЄС і Європарламент швидко ухвалити законопроекти з фінансовому нагляду, щоб Європейське управління з системних ризиків і три Європейські наглядові служби запрацювали на початку 2011 р.; домовитись із законопроектів щодо альтернативних менеджерів інвестфондів і щодо поліпшенню нагляду ЄС за кредитними рейтинговими агентствами; Єврокомісію підготувати пропозиції по ринках деривативів, особливо заходам з "коротких" продажів (включаючи незабезпечені) і свопах по кредитних дефолтах.

Для макроекономічного моніторингу необхідно розробити показники оцінки змін конкурентоспроможності і дисбалансів, що забезпечують раннє виявлення нестійких або небезпечних трендів, а також створити ефективну систему нагляду, що характеризує ситуацію в країнах Єврозони. Єврорада вирішила, що країни-члени повинні ввести системи податків і зборів на фінансові інститути для справедливого розподілу і обмеження системних ризиків.

Також слід чекати посилення координації економічної політики держав-членів. Комісія ставить наступні завдання: 1) виробити пропозиції про посилені заходи координації і нагляду за економічною політикою держав-членів; 2) ввести в дію ефективний механізм примусу, який гарантує те, що держави-члени виконуватимуть узгоджені у рамках ЄС рішення; 3) провести Семестр координації економічної політики, який допоможе їм освоїтися в новій ситуації.

Особлива роль у Стратегії відводиться новій промисловій політиці ЄС, у рамках якої здійснюватиметься подальша модернізація систем державних закупівель, державної підтримки й інших правил конкуренції, спрощення і інтернаціоналізація діяльності МСП, забезпечення ефективного доступу до єдиного ринку, розвиток європейської стандартизації, становлення інструментів для вирішення глобальних завдань і проектів, таких як "Галілео" і ГМЕД (Глобальна система моніторингу довкілля).

Незважаючи на логічність і чіткість, нова стратегія не виглядає дуже переконливою, зокрема при порівнянні головних цілей із переліком головних кількісних орієнтирів. До "розумного росту" відносять ріст витрат на НДДКР і підвищення частки молоді з вищою освітою. З "стійким ростом" зв'язані ріст зайнятості, скорочення парникових викидів, підвищення енергоефективності і ширше використання альтернативних джерел енергії. "Інклюзивний ріст" повинен вимірюватися часткою молодих людей, що завершили середню освіту, і чисельністю незаможних. Очевидно, що багато важливих складових нової стратегії, наприклад, конкурентоспроможність, інноваційність, територіальне зближення, ЄС не планує вимірювати кількісно. А раз так, то дізнатися про виконання або невиконання поставлених цілей буде неможливо.

Також у документі жодного разу не згаданий Європейський центральний банк, включаючи розділ 5.2, де розписані повноваження усіх виконавців стратегії. Комітет регіонів є, а ЕЦБ, що відповідає за головну опору ЄВС, немає. Немає його і в розділі про вдосконалення єдиного внутрішнього ринку, хоча саме ЕЦБ виконує основну, украй складну технічно, роботу із створення інтегрованого фінансового ринку Єврозони. Причини такої відсутності можна трактувати двояко. З одного боку, ЕЦБ є незалежним органом і не підкоряється рішенням Ради. Тому давати йому рекомендації або розпорядження некоректно. З іншого боку, неучасть ЕЦБ можна сприймати як ознаку наростаючої конкуренції між керівними органами ЄС. Це може розцінюватися також і як прояв слабкої координації між економічною і грошово-кредитною частинами ЄВС.

Висновки. Нові ініціативи у сфері економічного управління (economic governance) Євросоюзом мають бути вироблені до кінця року. Це складний процес, адже будь-які спроби посилити контроль Ради і ЄК над діями національних урядів у частині економічної політики і, тим більше, втрутитися в процес прийняття державних бюджетів, де головну роль відіграють національні парламенти, можуть привести до повторення кризи, що виникла в ході ратифікації Конституції ЄС. Показово і те, що багато експертів висловлюються проти використання терміну "економічне управління", вважаючи достатнім посилення координації економічної політики країн-членів.

1. Сайт Європейської Комісії. Електронний ресурс. – Режим доступу: http://ec.europa.eu/archives/growthandjobs_2009/documentation/index_en.htm#annual 2. "Європа 2020. Стратегія розумного, стійкого та інклюзивного росту" "Europe 2020. A strategy for smart, sustainable and inclusive growth" Електронний ресурс. – Режим доступу: http://ec.europa.eu/archives/growthandjobs_2009/ 3. Етапна доповідь про процес і реалізацію. Електронний ресурс. – Режим доступу:http://ec.europa.eu/growthandjobs/pdf/european-economic-recovery....december_2009_en.pdf). 4. Евростат. Електронний ресурс. – Режим доступу (http://epp.eurostat.ec.europa.eu).

Надійшла до редколегії 12.09.11

В. Морозов, канд. екон. наук, доц.

РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ ТОРГІВЛІ У ФРН

У статті розкрито основи сучасної системи регулювання електронної торгівлі у ФРН. Розглянуто найважливіші регуляторні механізми німецького законодавства та законодавства ЄС, які регламентують торговельну діяльність в Інтернет. Наведено і проаналізовано особливості функціонування відповідних уповноважених німецьких державних органів влади, серед них: "Відомство з регулювання телекомунікаційної та поштової діяльності ФРН", Федеральне відомство із забезпечення безпеки в сфері інформаційної техніки. З'ясовано новітні тенденції розвитку сфери електронної комерції у ФРН та ЄС.

The article explores the principles of the modern system of regulation of electronic commerce in Germany. It also analyses the most important regulatory mechanisms of German law and EU law governing the trading activities on the Internet. The analysis also covers the specifics in the functioning of the authorized German state bodies, among them: "Regulatory Authority for Telecommunications and Posts", "Federal Office for Information Security". The author outlined the latest development trends in the sphere of e-commerce in Germany and the EU.

Федеративна Республіка Німеччина (ФРН), як країна-член Європейського Союзу (ЄС), у своїй державній політиці у сфері регулювання електронної торгівлі, у цілому, та використання електронних документів з електронним

підписом, зокрема, керується нормами спільного європейського законодавства у цій сфері. Основна позиція ЄС щодо регулювання електронної комерції передбачає досягнення окремих результатів, – головним чином, розвиток однотипних законів у незалежних державах ЄС з відмінними правовими системами та традиціями.

У сфері регулювання електронної торгівлі в ЄС, на сьогодні, існують дві основні Директиви:

1. **Директива про електронну комерцію 2000 року** ***("ДЕК"*** *– англ. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce))* [1];

2. **Директива про електронні підписи 1999 року** ***("ДЕП"*** *– англ. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive)* [2].

"ДЕК" встановлює загальні основи для розвитку електронної комерції. Зокрема, стаття 9 Директиви вимагає від держав-членів ЄС надання законної сили договорам в електронному вигляді, усунення бар'єрів та перешкод для їх використання і забороняє заперечення їх чинності виключно на підставі їх електронного вигляду. Зобов'язання та вигоди, що випливають з "ДЕК", є дійсними тільки в межах ЄС.

"ДЕП" є більш деталізованою і встановлює основи для визнання електронних підписів та вимоги до держав-членів ЄС у сфері їх сертифікації. Так, стаття 5 "ДЕП" зазначає, що "електронні підписи, які виконані на основі кваліфікаційного сертифікату і створені за допомогою захисного засобу", – еквівалентні власноручним підписам. Однак, надалі в статті зазначено, що електронний підпис не може бути позбавленим чинності винятково на підставі того, що він був створений без використання кваліфікаційного сертифікату чи захисного засобу. Незважаючи на наявність таких визначень, текст Директиви залишається технологічно нейтральним: мета вимог полягає в гарантуванні досягнення максимального ступеню безпеки, замість вказування на конкретний пристрій чи метод створення електронного підпису.

Крім того, у статті 2 "ДЕП" міститься визначення т.зв. *"посиленого електронного підпису" (англ. "advanced electronic signatures")*, який повинен відповідати наступним вимогам:

1) бути пов'язаним безпосередньо з особою, яка підписала;

2) бути достатнім для її ідентифікації;

3) бути створеним за допомогою засобів, що знаходяться під одноосібним контролем особи, яка підписала;

4) бути пов'язаним з даними, до яких він відноситься, у такий спосіб, щоб будь-яка наступна зміна цих даних ставала очевидною.

Для перевірки електронного підпису використовується "сертифікат" ("кваліфікаційний сертифікат" – п.п. 9,10 ст. 2 Директиви). Сертифікат являє собою електронне посвідчення, що пов'язує дані для перевірки електронного підпису з визначеною особою та підтверджує ідентичність цієї особи. Кваліфікаційний сертифікат являє собою сертифікат, що відповідає спеціальним вимогам, які описані у Додатку І Директиви, та виданий органом сертифікації, який відповідає вимогам Додатку ІІ Директиви.

Німецький підхід до надання чинності торговельним договорам в електронному вигляді в частині встановлення вимоги щодо власноручного підпису полягає у встановленні *достатньо жорсткого режиму державного регулювання*. При цьому, одним з найскладніших питань регулювання електронної комерції є використання електронного цифрового підпису. Саме тому у ФРН, як і в переважній більшості інших країн-членів ЄС, це питання врегульоване окремим законом.

Зокрема, у 1997 р. набрав чинності "**Закон про цифровий підпис ФРН"**, що є статтею 3 "*Закону про регулювання основних умов надання інформаційних і комунікаційних послуг" (нім. Informations- und Kommunikationsdienstegesetz)* [3]. Невдовзі анульований, даний Акт надав чинності електронним підписам в електронній комерції.

Додаткові технічні вимоги були закріплені у тому ж році у "**Постанові про цифровий підпис"** *(англ. Digital Signature Ordinance)* [4].

Дані нормативні акти, по-суті, сформували регулятивну основу для створення і підтвердження цифрових підписів органами сертифікації, що мають державну ліцензію. Останніми роками у ФРН відбувається процес регулювання використання криптографії з відкритим/закритим ключем, в рамках якого встановлюються технічні вимоги до органів сертифікації, які повинні цілком відповідати Закону – з метою одержання дозволу на здійснення діяльності. Основний наголос Закону зроблений на створенні т.зв. інфраструктури цифрових підписів, а не на визнанні чинності договорів в електронному форматі. Нежиттєздатність даної спроби обумовлюється відсутністю специфічних положень, що стосуються дійсності та сфери використання цифрових підписів в електронних угодах. Замість цього даний закон містить технічні норми-вимоги до органів сертифікації, яким вони повинні задовольняти для отримання ліцензії.

Враховуючи той факт, що офіційне визнання чинності електронних документів, – рівної паперовим, – не гарантується Законом, як це зроблено в "ДЕК", мають місце *дві основні проблеми гармонізації німецького регуляторного законодавства.*

По-перше, відсутність офіційного законодавчого визнання електронних документів зумовлює необхідність надання додаткових коментарів і пояснень стосовно сфери дії угод. На даний час існує велика кількість законодавчих вимог, яким не задовольняють електронні та цифрові підписи. Таким чином, визначення угод, які можуть укладатись в електронному виді, вимагає аналізу законодавства і, як наслідок, збільшення вартості угоди.

Друга проблема створена відповідно розділами 14 і 15 Закону, які визначають механізм застосування стандартів цифрового підпису для іноземних органів сертифікації. Зокрема, цифрові підписи, створені органом іншої держави-члена ЄС, можуть бути визнані тільки у тому випадку, якщо вони мають та можуть довести відповідний рівень безпеки. Проте, як його можна довести – не зовсім зрозуміло. При цьому, як правило, вимагаються схожі умови тестування та регулюючий режим для відповідності даному Положенню. Для держав – не членів ЄС підрозділ 15(2) зазначає, що цифрові підписи можуть визнаватись рівноцінними тільки при наявності відповідних міжнародних чи міжурядових договорів.

Недоліки та надмірна негнучкість стандартів, що містяться в німецьких законодавчих ініціативах 1997 року, суперечили, по-суті, вимогам двох Директив ЄС. Тому уряд Німеччини розробив додаткові акти для заміни існуючого Закону і подальшої "інтеграції" з "ДЕП" [5, 6]. Серед них слід назвати:

1. Німецьку пропозицію по основах "Закону про цифрові підписи" від 16 серпня 2000 року, прийняту Бундесратом в якості Постанови 9 березня 2001 року [7];

2. Т.зв. "**Закон про підпис"** *(нім. "Signaturgesetz – SigG")*, який набрав юридичної чинності 21 травня 2001 року [8]. При цьому "SigG" не ставить знак рівності між електронними і власноручними підписами; точніше

він створює основи для відповідності "ДЕП". Одночасно, все-таки, залишається обов'язковий набір правил для створення і випуску сертифікатів, що можуть бути визнаними відповідно до Директиви; однак електронні підписи, за визначенням, є самодостатніми для того, щоб бути своєрідним доказом укладання угоди в електронній формі. Перша частина Закону формулює мету всього Акту: формування основ для електронних підписів. Здавалося б, вона набагато більше відповідає Директиві, ніж у попередньому Законі. Проте, замість регулювання сфери дії електронних підписів, Закон продовжує формування механізму інфраструктури цифрових підписів.

Наприкінці 2005 р. завершився процес підготовки до внесення змін до статті 126(а) "Цивільного кодексу ФРН", які б гарантували законний статус кваліфікаційного сертифікату [9]. До того ж, визнання іноземних сертифікатів є можливим за умови, якщо закордонні органи сертифікації, що їх видали, пройшли акредитацію і можуть забезпечити відповідний рівень безпеки (згідно Статті 1 § 6(23)). У випадку, якщо відповідні законодавчі зміни будуть мати місце, – це створить гарантії використання електронних підписів у всіх сферах господарської діяльності ФРН незалежно від того, для чого використовуються дані підписи.

Новий і удосконалений "SigG", деякою мірою, пом'якшив позицію Німеччини у сфері регулювання використання електронних документів з електронним підписом, але не забезпечив повною мірою створення ефективного законодавства щодо законного визнання договорів в електронному вигляді.

Так, відповідно до німецького законодавства, під **центром сертифікації** *(нім. Zertifizierungsstelle, англ. certification authority, у німецько- та англомовній, а іноді й російськомовній літературі використовуються також терміни "Trust Center і Trustcenter")* розуміється "фізична чи юридична особа, яка засвідчує зв'язок відкритих ключів підпису з визначеною фізичною особою і має ліцензію відповідно до § 4 діючого Закону "SigG" [10].

На центри сертифікації покладені основні задачі забезпечення функціонування технології цифрових підписів:

- створення ключів,
- посвідчення особи їхніх власників (персоніфікація),
- сертифікація,
- ведення реєстрів користувачів ("служба каталогів"),
- посвідчення документів за допомогою оцінки часу.

Для вирішення питань безпеки передбачена сувора процедура ліцензування діяльності центрів сертифікації, що проводиться урядовими службами. Центр сертифікації може отримати ліцензію тільки в тому випадку, якщо доведеною є його здатність виконувати запропоновані Законом і Постановою норми безпеки, і надалі урядові органи зобов'язані регулярно проводити перевірки дотримання центром сертифікації вимог безпеки. У випадку, якщо діяльність Центру перестане відповідати вимогам безпеки, і недоліки не будуть цілком усунуті протягом встановленого урядовим органом терміну часу, – ліцензія повинна бути скасованою. На відповідну урядову службу ФРН покладений обов'язок ведення бази даних з інформацією про всі ліцензовані центри сертифікації, зокрема з інформацією про їх публічні ключі сертифікації.

Видача ліцензій центрам сертифікації та видача сертифікатів, що використовуються центрами для підписання сертифікатів, а також нагляд за дотриманням положень "Закону про цифровий підпис" і "Постанови про цифровий підпис", згідно "Закону про цифровий підпис", відноситься до компетенції уповноваженого державного органу Німеччини, зазначеного в §66 "Закону про телекомунікації", тобто "**Відомства з регулювання телекомунікаційної та поштової діяльності ФРН"** *(нім. Regulierungsbehoerde fuer Telekommunikation und Post).* З його організаційною структурою, створеною для забезпечення ефективної діяльності з надання послуг електронного підпису, можна ознайомитись в Інтернеті за адресою: *http://www.regtp.de/behoerde/start/in_01-01-00-00-00_m/fs.html* [11].

Згідно абз. 5 §4 "Закону про цифровий підпис" уповноважений державний орган видає сертифікат для ключа підпису, що використовується центром сертифікації для підписання сертифікатів. Таким чином створюється ієрархія сертифікатів. Держорган своїм підписом засвідчує підпис центру сертифікації, а останній, у свою чергу, своїм підписом засвідчує підпис кінцевих користувачів. Розпорядження про видачу сертифікатів центрами сертифікації діють також для уповноваженого державного органу, що видає сертифікати для центрів сертифікації.

Він зобов'язаний за допомогою загальнодоступних засобів телекомунікації забезпечувати постійний публічний доступ до виданих таким центром сертифікатів, а також до інформації про адреси та телефонні номери відповідних центрів сертифікації, інформації щодо призупинення дії таких сертифікатів, про припинення діяльності центрів сертифікації та про термін дії виданих ліцензій.

Центр сертифікації для цифрових підписів при "Відомстві з регулювання телекомунікаційної та поштової діяльності ФРН" розпочав свою роботу 23 вересня 1998 р. у м. Майнц [12].

З інформацією стосовно джерел, обсягів фінансування створення даної організаційної структури Німеччини щодо надання послуг електронного підпису та електронного документообігу, а також з конкретним механізмом сплати за послуги з видачі сертифікатів ключів та ін. організаційно-правовими аспектами можна ознайомитись в Інтернеті за адресою: *http://www.regtp.de/behoerde/*.

Необхідно зазначити, що на сьогоднішній день для чиновників Федерального Уряду Німеччини вже введено в дію механізм електронного підпису. Понад 200 тис. працівників міністерств і відомств мають можливість підписувати електронні документи за допомогою т.зв. "смарт-карти", що містить зашифрований ключ. За сферою чинності електронний підпис прирівнюється до звичайного.

Видаче карт та пристроїв їхнього зчитування у ФРН було завершено наприкінці 2005 р., коли закінчилась робота над проектом по забезпеченню виходу 400 державних служб Німеччини в Інтернет. Близько чверті цих служб вимагають у своїй діяльності наявності електронних підписів. У рамках проекту були розроблені стандарти захисту електронних трансакцій, документів, доступних через Інтернет, та електронної пошти. Зокрема, при фінансовій підтримці Уряду ФРН завершено розробку і здійснено впровадження стандартів *"Industrial Signature Interoperability Specification" і "MailTrus"*.

Одночасно хотіли б звернути увагу на той факт, що значний інтерес у свій час викликав також документ під назвою **"Офіційна позиція німецького Уряду щодо міжнародного визнання електронних цифрових підписів"** *(англ. German Government Position Paper on the International Recognition of Digital Signatures)*. Даний документ не вважається офіційним нормативно-правовим актом, однак дозволяє "підсумувати" дії німецького Уряду і визначити його загальну позицію у сфері регулювання використання електронних документів з електронним цифровим підписом в органах влади [13].

По-перше, для Німеччини у сфері регулювання використання електронних документів з електронним ци-

фровим підписом в органах влади на першому місці знаходяться такі поняття, як надійність та безпека електронних підписів. Це проглядається ще раз в Акті про електронний цифровий підпис: *"... спочатку потрібно створити систему сертифікації підписів, а потім вже вести роботу по зрівнянню електронних цифрових підписів із власноручними."*

По-друге, пріоритетом є не "bona fide" сторін, а державний контроль за використанням підписів. Відповідно, й визнання електронних підписів можливе лише в умовах жорсткої бюрократичної системи їх сертифікації.

По-третє, у даному випадку німецький Уряд не може допустити визнання іноземних підписів, що не відповідають внутрішнім стандартам: велика "дірка на кордоні" зробила б безглуздою сувору внутрішню сертифікацію. Власне кажучи, це і зазначено в п.1 §15 "Акту про електронний цифровий підпис" ("ЕЦП"), вірогідність якого може бути перевірена за допомогою відкритого ключа, сертифікованого в "іншій державі", може бути визнана еквівалентною "ЕЦП" за дійсним Актом, якщо він має такий самий рівень безпеки".

Подібна жорсткість державного регулювання сфери використання електронних документів з електронним цифровим підписом фактично створює т.зв. "ілюзію залізної завіси" навколо Німеччини, крім її участі в міжнародній електронній комерції. Подолати цей бар'єр можливо тільки в тому випадку, якщо німецькі стандарти електронних підписів стануть загальними, що є на сьогодні малоймовірним. Іншими словами, даний підхід до державного регулювання використання електронних підписів у ФРН виключив можливість вирішення головного завдання впровадження електронних підписів – інтернаціоналізації електронної комерції.

Протягом останніх років державні органи ФРН активно працювали над реалізацією свого наміру щодо криміналізації "спамерства" у Німеччині. Згідно зі зробленими заявами, введення лише штрафів не достатньо, і розповсюдження "спаму" має кваліфікуватись як злочин, за який передбачено покарання або ув'язнення. Робоча група з питань телекомунікацій і поштової кореспонденції ще не вирішила питання про тривалість строку бажаного покарання. Німеччина має намір ввести "антиспамове" законодавство до окремого закону проти недобросовісної конкуренції, який також забороняє нав'язане розсилання факсів *(англ. "unsolicited faxing")*, а не до "Закону про телекомунікацію", одночасний перегляд якого очікується найближчим часом.

На думку німецьких урядовців, покарання позбавленням волі є обов'язковим для того, щоб зупинити найбільших "спамерів", які розсилають мільйони небажаної поштової реклами. Є підозра, що 2 або 3 найбільші "спам ери" за рейтингом "TOP-50" походять саме з Німеччини. Проте, окремі опозиційні партії не бажають вводити кримінальне покарання і пропонують зупинитись на адміністративних штрафах. Як і багато інших країн ЄС, Німеччина не імплементувала нове європейське "антиспамове" законодавство вчасно.

Крім того, з кінця 2003 р. у Німеччині вступив у дію новий закон, що захищає власників авторських прав в Інтернеті.

Відтепер власники сайтів, на яких викладені авторські твори, можуть бути покарані. Новий закон не відмежовує тих, хто і з якими цілями займається незаконним поширенням ліцензійної продукції, – юридичну чи приватну особу; не враховує той факт, чи отримується від цієї діяльності прибуток чи ні. Відтепер навіть приватний перегляд незаконно скопійованого фільму в колі родини може вважатися незаконним.

Стрімка комп'ютеризація суспільства у ФРН та інших країнах ЄС, поява нових, раніше невідомих злочинів в сфері комп'ютерної інформації, виявили, що правоохоронні органи неготові до адекватного протистояння й активної боротьби з цим новим соціальним явищем. Так, наприклад, у ФРН було виявлено 2,7 тис. випадків аналогічних злочинів, з них розкрито тільки 170, тоді як інші 2,53 тис. кримінальних справ було припинено за різними обставинами; у Великобританії з 270 встановлених злочинів з використанням засобів комп'ютерної техніки за останні 5 років було розкрито тільки 6; у Франції зареєстрованих налічувалось 70 злочинів, а розкрито тільки 10 кримінальних справ; у США за цей же період правоохоронними органами було розкрито 200 злочинів, за якими до кримінальної відповідальності було притягнуто лише 6 осіб.

Результати проведеного дослідження та аналіз статистичних джерел інформації показують, що приблизно 80-90% скоєних у ФРН комп'ютерних злочинів, залишаються невідомими для правоохоронних органів. Наведені дані красномовно свідчать про рівень складності здійснення процесів розслідування злочинів категорії, що розглядається.

Строки покарання за такі дії у залежності від небезпечності злочину у різних країнах визначаються порізному: у Німеччині за менш небезпечні факти "відмивання" грошей передбачено 5 років ув'язнення, за важкі – 10, у Швейцарії – відповідно 2 роки і 10 років. У Великобританії двома роками позбавлення волі карається також відсутність у фірми заходів щодо процедури викриття фактів "відмивання" грошей, здобутих злочинним шляхом.

Слід підкреслити, що при покаранні злочинців з фінансових установ за "відмивання" грошей правоохоронним органам не потрібно доводити, що гроші були здобуті злочинним шляхом, тобто карається сама процедура неналежної перевірки прийнятих від вкладника грошей.

Підбиваючи підсумки характеристики злочинів, що можуть здійснюватись з використанням системи Інтернет-торгівлі, слід ще раз підкреслити важливість невідкладної розробки і прийняття законодавчих актів з питань "відмивання" фіктивно утворених грошових коштів, грошей, здобутих злочинним шляхом, та використання комп'ютерних систем для скоєння розглянутих та інших економічних злочинів. Втім, "жорсткий" підхід до регулювання питань електронної комерції та застосування електронних підписів характерний не для всіх країн-членів ЄС.

Окремо хотіли б наголосити на тому, що організаційно-законодавче регулювання електронної комерції у ФРН, а саме використання електронних документів з електронним підписом, тісно пов'язане з питаннями захисту інформації у ФРН у цілому.

Німецьке законодавство в галузі захисту даних засноване на положеннях, які ґрунтуються на принципі інформаційного самовизначення. Таким чином, кожний громадянин, у принципі, сам розпоряджається своїми особистими даними. Якщо в інтересах суспільства він, – наприклад, як платник податків – змушений відкрити цю інформацію, то питання державних установ до нього повинні обмежуватися необхідним мінімумом.

Використання особистих даних громадян у Німеччині заборонено. У виняткових випадках діють жорсткі законодавчі обмеження *(т. зв."Заборона із можливістю отримання дозволу")*. Інформацію про громадян дозволяється збирати і використовувати тільки в рамках чітко обмежених цілей.

Кожен громадянин має право на інформацію про те, як заклади, які опрацьовують особисті дані, використовують відомості про нього. Якщо в людини склалося враження

про незаконне використання її особистих даних, вона може звернутися за допомогою до Уповноваженого із захисту даних. Відповідна директива ЄС 1995 р. ще більше розширила інформаційні права громадянина.

Відповідна *Директива 95/46/EG*, прийнята в жовтні 1995 р., вимагала включити ці норми в національне законодавство протягом трьох років [14]. Деякі країни, включаючи Німеччину, не змогли дотриматися цього терміна. Проте, норми, що регулюють взаємовідносини між громадянином і державою, уже зараз мають пряму дію, без участі національних законодавців, тому кожний громадянин може безпосередньо посилатися на права, котрі чітко визначені і гарантовані в Директиві ЄС.

Це, насамперед, стосується принципової заборони на обробку так званої "чутливої" інформації. При цьому маються на увазі всі відомості, що стосуються расового та етнічного походження, політичних і світоглядних поглядів, здоров'я і сексуального життя. Так, наприклад, відомості про стан здоров'я робітника не можуть без його згоди бути передані роботодавцю.

Крім того, Директива набагато ширше трактує право громадян знати про те, як використовуються їх особисті дані, і оскаржити їхнє неправомірне використання, ніж це гарантує Федеральний закон про захист даних 1991 р. Громадянин, наприклад, має право знати, які державні установи мають доступ до його особистих даних. Захисту підлягають тепер також тимчасові банки даних.

Крім того, Директива зобов'язує національних законодавців підсилити захист особистих даних громадян від використання цих даних приватними закладами, насамперед приватними комерційними Інтернет-фірмами. Якщо хтось збирає особисті дані громадянина, то він зобов'язаний оповістити його про це і повідомити, що станеться далі з цією інформацією.

У зв'язку з цим, звернемось до **хронології розвитку цією проблематики**. Слід зазначити, що система захисту даних була створена в Німеччині близько тридцяти років тому. Німецькі фахівці із захисту даних не знайшли в жодній іншій країні відповідних законодавчих моделей. Вони стали першопрохідниками в цілком новій галузі регуляторної політики. На основі споконвічно суто технічних і організаційних заходів для запобігання незаконного використання інформації, зібраної в автоматичних банках даних, вони згодом розробили право кожної людини на захист від цікавості навколишніх, що рівносильне основному праву людини і тому діють майже без обмежень.

Найперша регуляторна норма в галузі захисту даних не тільки у ФРН, але і в усьому світі була прийнята в 1970 р. Висунуту Федеральною землею Гессен ініціативу через якийсь час підтримали інші федеральні землі. Федеральний закон у згаданій галузі діє з 1977 р. Шість років потому Федеральний конституційний суд, вища судова інстанція Німеччини, встановив ще одну важливу віху на цьому шляху. З тих пір основним критерієм використання особистої інформації в громадському управлінні та у приватному опрацюванні даних є інформаційне самовизначення кожного громадянина: громадяни самі приймають рішення про розголошення і використання інформації, котра стосується їх особисто.

В основі розвитку системи захисту даних лежало політико-психологічне прагнення перебороти настороженість громадян стосовно державного планування та його інструментів, що призвело до розробки – спочатку ненавмисного – нового індивідуального регуляторного механізму конституційного рівня.

Земельний уряд Гессена розробив законопроект про захист даних в галузі адміністративного управління. Цей закон переслідував *дві цілі*: він повинний був, *по-перше*, запобігти вторгненню в приватну сферу громадян за допомогою нової інформаційної техніки; а *по-друге*, не допустити зміни визначеного Конституцією розподілу повноважень у зв'язку з "інформаційною перевагою", яка виникала у виконавчих органів влади перед парламентськими органами.

З тих пір будь-який громадянин може звернутися зі скаргою до обраного Ландтагом і незалежного Уповноваженого із захисту особистих даних громадян. Саме він, як вважав Уряд, повинний був позбавити громадян відчуття, що вони знаходяться в залежності від оснащеної сучасною технікою бюрократії.

Прийнятий у Гессені закон стосувався тільки захисту особистих даних громадянина від втручання держави. Такі питання, як захист даних громадянина "А" від громадянина "Б", даних автолюбителя від цікавості страхової компанії або даних працівника від зазіхань його роботодавця в земельному законі залишалися відкритими через розподіл компетенцій між землями і федерацією.

У галузях, що виходять за рамки державного управління, тобто в приватній економіці і громадському житті, компетенція прийняття законів належить федеральному центру. Саме він відповідає за зберігання правової та економічної єдності Німеччини, тому що розходження між нормами, прийнятими в землях, скоріше заважають цій єдності. Обговорення проекту *Федерального закону про захист даних*, який стосувався як органів федерального управління, так і кожного громадянина, почалося ще в 1971 р. Але прийняти цей закон вдалося тільки через шість років. Тривалість дискусій пояснювалася – принаймні, частково – тим, що мова йшла про цілком нову сферу регуляторної діяльності. Особлива проблемність полягала в тому, що держава мала намір втрутитися у відношення, які до цього визначалися волею громадян, тобто були частиною їх "приватної автономії".

Подальший напрямок розвитку було вказано підготовленим на замовлення Уряду в 1971 р. науковим дослідженням про *"Основні проблеми захисту даних"*. Автори дослідження висунули тезу про те, що потоки інформації створюють свого роду нервову систему людського співіснування, а володіння інформацією про співгромадян являє собою "соціальне насилля". Автоматична обробка даних означає "широкомасштабне усунення міжлюдських кордонів і перепон" в галузі використання інформації і тому являють собою нову загрозу для рівноправності громадян.

Такому збору даних автори дослідження протиставили "право громадян на інформаційне самовизначення". Це означає, що кожен має сам визначати, у якому обсязі держава або співгромадяни повинні мати інформацію про його дії і думки. У коментарі до Федерального закону про захист даних говориться, що "право бути залишеним у спокої", повідомляти або приховувати інформацію є основним правом, яке випливає із закріпленого в Конституції права на вільний розвиток особистості.

Захищаючи одне з основних прав громадянина, принцип інформаційного самовизначення, в той же час, обмежує основне право його співгромадян на фаховий і економічний розвиток: власник Інтернет-магазину канцтоварів і шкільних посібників, звичайно, зацікавлений у тому, щоб мати дані про всіх першокласників, знати їхні адреси, а, по можливості, і фінансові можливості їхніх батьків. Однак при цьому, на думку авторів дослідження, необхідно завжди враховувати "потенційну небезпеку інформаційних систем". Тому "конфлікт інтересів вирішується, у більшості випадків, на користь приватної інформаційної системи". А використання даних про громадян, які отримані не із загальнодоступних джерел, необхідно

заборонити в принципі, дозволяючи його тільки у виняткових випадках, визначених нормативними актами.

Федеральний закон про захист даних увібрав у себе велику частину цих положень. Він дозволив обробку даних тільки у випадках, визначених законом, або за згодою громадянина, що дає йому можливість проконтролювати цей процес.

Через дванадцять років після обґрунтування вченими права на "інформаційне самовизначення" воно було також визнано вищою судовою інстанцією країни. Федеральний конституційний суд заявив у 1983 році: "Той, хто не знає з достатньою певністю, які дані, що його стосуються, відомі у певних сферах його соціального оточення, і хто не в змозі приблизно оцінити об'єм інформації, яким володіють його можливі партнери по комунікації, може бути значною мірою ущемлений у своїй свободі планувати і приймати рішення на основі самовизначення. З правом на інформаційне самовизначення були б несумісні громадський порядок і правовий порядок, який служить йому основою, при яких громадянин не міг би знати, хто, що, коли і за яких обставин про нього знає (...). Звідси випливає: вільний розвиток особистості в сучасних умовах обробки даних припускає наявність захисту індивідуума від необмеженого збору, накопичення, використання і поширення його особистих даних (...). Основне право (розвиток особистості) гарантує (...) право кожного самостійно приймати рішення про розголошення і використання його особистих даних".

Для цього необхідно, насамперед, гарантувати прозорість потоків інформації: дані про громадян не повинні проходити через сумнівні канали, люди, яких це стосується, повинні мати можливість контролювати проходження цієї інформації. Тому головними критеріями будь-якого використання інформації є необхідність і ціль такого використання.

Приміром, якщо подружжя під час шлюборозлучного процесу повідомляють суду у сімейних справах про свої прибутки, то ці відомості можуть використовуватися тільки в рамках процесу, вони не повинні потрапляти, наприклад, у податкові служби, які завжди жваво цікавляться економічним становищем громадян. Цілком несумісним із принципом цільового використання інформації був би, наприклад, "центральний реєстр" усіх жителів, яким у випадку потреби могли б користуватися і поліція, і управління народного освіти, і відомство у справах іноземців, і, навіть, Інтернет-торговці. Такий збір даних є неприпустимим.

Рішення Вищого німецького суду, що стало вже класичним, стосувалося захисту особистих даних громадянина від втручання держави. Конкретно ж воно було пов'язано з переписом населення. При цьому досить загальні формулювання із самого початку торкалися також і приватного сектору.

Нова редакція Закону про захист даних, прийнята в 1991 р., була покликана протидіяти не тільки неправомірному використанню особистих даних громадян. З урахуванням роз'ясненого конституційним судом принципу інформаційного самовизначення Закон спрямований на те, щоб "захистити кожного громадянина від обмеження його особистих прав у результаті використання (іншими) його особистих даних". Використання особистих даних припускає згоду даної особи або повинне бути дозволене законом.

Згідно з *Першим федеральним законом* (1977 р.) захист даних починав діяти при існуванні банку даних. У новій редакції захист даних починається вже при зборі, тобто при цілеспрямованому одержанні інформації про громадян. При цьому, у приватній сфері – наприклад, в економічному житті – діють такі загальні правила цивільних правових відносин, як сумлінність і правова поведінка. Контроль за дотриманням цих правил можуть здійснювати наглядові органи федеральних земель.

Держава також у принципі не має права збирати ніяких відомостей "за спиною" громадянина. Під захист даних підпадають, насамперед, персональні справи і всі офіційні процедури, у тому числі ті, які включають в себе відео- і аудіозаписи (зроблені, наприклад, поліцією).

У приватній сфері, щоправда, банк даних, в загальному і цілому, залишився тим порогом, з якого починає діяти захист зібраних даних. Всі інші відомості про людей – наприклад, списки, книги або "страхові документи" – знаходяться поза сферою захисту.

Відповідно до нової редакції Закону, прийнятої в 1991 р., самі дані знаходяться під захистом лише тоді, коли вони застосовуються не тільки в приватній сфері, а виконують якусь функцію в суспільному та економічному житті. Межа стає більш чіткою на одному прикладі, що використовують, зокрема, контрольні органи федеральних земель: список днів народження друзів і знайомих не підпадає під захист даних на відміну від такого списку, складеного якоюсь організацією для своїх членів. Метою законодавця була не регламентація будь-якого обміну інформацією в колі близьких знайомих, а, скоріше, захист приватної сфери кожного громадянина в рамках загальної мережі контактів, які все більше стають безособовими, як, наприклад, у відносинах між організацією і її членами.

Закон регламентує використання особистих даних громадян в економічному і громадському житті в залежності від того, для яких цілей зібрана подібна інформація – в інтересах власного бізнесу або ж за завданням іншої особи. Власні цілі переслідує при цьому, наприклад, приватна медична фірма або адвокатська контора, які створюють власну інформаційну систему в інтересах своєї справи (наприклад, збираються дані про пацієнтів і клієнтів); при цьому інформаційне Інтернет-бюро у фінансово-економічній сфері, яке передає наявні в неї відомості третім особам в інтересах їхнього бізнесу, тобто виступає тільки в якості передавача інформації, підпадає під другу категорію.

В галузі обробки даних по (чужому) завданню діють в основному ті ж правила, як і у випадку використання інформації у власних цілях. Проте, такі організації повинні бути зареєстровані в контрольних органах, вони повинні ставити їх до відома про наявні у їхньому розпорядженні технічні засоби і у випадку регулярної передачі даних про громадян надавати інформацію про одержувачів цих даних.

Громадські і приватні установи повинні за вимогою громадянина інформувати його про те, які дані про нього, що підпадають під захист, вони мають в своєму розпорядженні. Це стосується також відомостей про джерело інформації і її отримувача. Ця інформація повинна надаватися письмово, у ясній формі і безкоштовно.

Приватна особа, яка збирає в інтересах своєї справи дані про інших осіб, які не являються загальновідомими, наприклад, для надання кредиту, повинна проінформувати про це особу, яку це стосується, якщо вона ще не дізналося про це – наприклад, із формуляру договору. Таким чином, кожний громадянин може, у принципі, дізнатися, які дані про нього поширюються в суспільстві.

Поряд із можливостями, які Закон надає кожному окремому громадянину для перевірки своїх даних, він передбачає також наявність контрольних інстанцій. Закон ставить за обов'язок федеральним адміністративним органам забезпечити захист інформації в сфері,

на яку поширюються їхні повноваження. Поряд із внутрішнім контролем закон передбачає також зовнішній контроль. Здійснення зовнішнього контролю в сфері суспільного управління входить до обов'язків Федерального уповноваженого із захисту даних. Його обирає Німецький Бундестаг. Обрання парламентом наділяє його власними демократичними повноваженнями і робить його значною мірою незалежним від державної адміністрації. Федеральний уповноважений із захисту даних обирається на п'ять років і може бути переобраний ще на один термін. Федеральний уповноважений нікому не підпорядковується і керується тільки Законом.

Одне з основних завдань Федерального уповноваженого полягає в тому, щоб перевіряти особисті скарги громадян на використання їх особистих даних федеральними державними установами та інформувати особу, яка подала скаргу, про результати перевірки. Він має право відмовитися від дачі показань у якості свідка, у тому числі в суді, і не зобов'язаний показувати свої робочі документи ніяким третім особам. Тому громадяни можуть довіритися головному захиснику даних у Федерації, не побоюючись витоку будь-яких відомостей.

Раз на два роки Федеральний уповноважений подає Німецькому Бундестагу звітну доповідь про свою діяльність; в ній він повинен також відобразити розвиток системи захисту даних у недержавній сфері. Можливість виступати в парламенті з критикою і пропозиціями дає йому прекрасний шанс впливати на громадську думку демократичного суспільства.

Кожне підприємство, на якому зайняті, як мінімум, п'ять робітників на автоматизованій або двадцять осіб на ручній обробці особистих даних, повинне мати власного Уповноваженого із захисту даних. Він підпорядковується безпосередньо керівництву і більше нікому в ієрархічній структурі підприємства. Уповноважений із захисту даних на підприємстві не виконує нічиїх вказівок і може бути відкликаний тільки в тому випадку, якщо цього зажадає контрольна інстанція, або якщо роботодавцю вдасться звільнити його через суд через серйозні промахи в роботі.

Порушення норм захисту даних може переслідуватися законом. Кримінально-правовий захист поширюється на дані, які не являються надбанням громадськості, такі, наприклад, як дані про стан здоров'я. Той, хто піддає такого роду інформацію автоматичному опрацюванню, не маючи на це право, тобто, приміром, записує її в пам'ять комп'ютера, передає її, витягує її з пам'яті комп'ютера або добуває таку інформацію ще якимось чином з банку даних, порушує Закон. Покарання загрожує також тому, хто домагається передачі даних обманним шляхом за допомогою хибних відомостей; хто передає їх, неприпустимим чином змінюючи ціль використання інформації, або протизаконно збирає дані.

Порушнику загрожує позбавлення волі терміном до одного року або грошовий штраф. Якщо він використовує інформацію з метою збагачення або намагаючись нашкодити іншій особі, то може бути позбавлений волі терміном до двох років. Такий злочин переслідується, однак, тільки за заявою потерпілого.

Зазначаючи **новітні тенденції розвитку сфери електронної комерції у ФРН, зокрема, та ЄС, у цілому**, слід вказати на той факт, що паралельно зі звільненням інформаційних потоків на внутрішньому ринку країн-членів ЄС підсилюється контроль над інформаційним обміном з країнами, які не входять до ЄС, так званими третіми країнами. До них, не в останню чергу, відносяться США. Сполучені Штати та ЄС пов'язані між собою найважливішими у світі потоками товарів та інвестицій. На відміну від державного регулювання в країнах ЄС, США в галузі захисту даних роблять ставку на саморегулювання економіки, головним чином на договірній основі. Європейська комісія та Уряд США шукають компромісне рішення. При цьому, для всіх країн-партнерів по ЄС обов'язковим залишається наявність контрольного органу, до якого потерпілі можуть звернутися без особливих зусиль і великих витрат".

В *галузі розробки програмного забезпечення* вигідним вважається перенесення цілих галузей виробництва в країни з дешевою робочою силою за межами ЄС *(англ. "Global Sourcing")*. Треті країни повинні мати відповідний рівень захисту при передачі даних. Його можна забезпечити за допомогою добровільних зобов'язань зацікавлених підприємств; такого роду регулюванню віддають перевагу, наприклад, у США. Рівень захищеності даних диктується, наприклад, їхнім характером (відомості з телефонних книг або виписки з банківських рахунків). У сумнівних випадках рішення приймає комісія, до якої входять представники країн-членів ЄС.

У випадку згоди зацікавленої особи з "експортом" його даних рівень захисту інформації в третій країні не має великого значення.

Взаємодію національних контрольних органів забезпечують спеціалісти країн-членів ЄС у рамках спеціальної *"Групи із захисту даних"*. Експерти щорічно подають на розгляд Європейської комісії, Європейського парламенту і Ради глав держав і урядів доповідь "Про рівень захисту фізичних осіб при обробці особистих даних у Європейському Союзі та у третіх країнах".

Спеціальний закон ФРН "Про інформаційні і телекомунікаційні служби" регулює відносини між фірмами, які пропонують телекомунікаційні послуги, та їх користувачами, наприклад у сфері телебанкінгу і телешопінгу. Клієнту повинна бути надана можливість скористатися цими послугами та оплатити їх анонімно, по можливості за допомогою оплаченої готівкою чіп-карточки, щоб ніхто інший не міг дізнатися, чим він цікавиться. Фірми можуть вимагати надання особистих даних тільки у тому випадку, якщо вони необхідні для укладення договору з клієнтом. Додаткову інформацію вони можуть одержувати тільки за згодою самого клієнта. При цьому Закон захищає споживача від кожної поспішно даної згоди, до чого його може підштовхнути вимога на екрані персонального комп'ютера (достатньо відповісти "Так" одним натисканням клавіші або мишки): підтвердження повинно бути запитане повторно, і цей запит повинний бути добре помітний на екрані. Закон однозначно визначає, що телекомунікаційні фірми можуть рекламувати свої послуги за допомогою підготовлених незалежними експертами висновків про прийняті ними заходи для захисту даних.

Подібний "аудит захисту даних" у сфері електронної комерції може до того ж стати гарним ринковим стимулом для забезпечення високого рівня захисту даних у всіх сферах життя. На користь цього в 1998 р. висловилося й Об'єднання німецьких юристів.

Федеральний уповноважений із захисту даних здійснює відповідний контроль над "транспортним рівнем" телекомунікацій, тобто над "власниками телекомунікаційних мереж"; у той час як контроль за "товаром", що поширюється по цих мережах, тобто за конкретними телекомунікаційними послугами, входить у компетенцію органів нагляду в недержавній сфері.

Проблеми розмежування повноважень в наявності: вони в принципі ставлять під питання необхідність подальшої "специфікації" захисту даних. Так, наприклад, виникає питання про те, чи являється сервер електронної пошти звичайною мережною телекомунікаційною послугою, тобто являє собою просте використання ком-

п'ютерної мережі, або ж його варто вважати самостійним видом змістовної телекомунікації, оскільки він одночасно пропонує послуги пошукової Інтернет-системи. Проте, хто б не відповідав за контроль: очікування, у тому числі й економічні, пов'язані з технічними нововведеннями, виправдаються тільки в тому випадку, якщо споживачі зможуть їм довіряти. А для цього необхідний надійний захист даних.

Федеральний закон про захист даних містить декілька положень, відповідно до котрих доступ до техніки, яка обробляє дані, робота на ній і використання накопиченої інформації дозволяються тільки певному колу осіб і підлягають контролю. Ці вимоги сформульовані, однак, в досить загальній формі, щоб умови збереження даних могли бути модифіковані в залежності від конкретних умов і технічного прогресу.

При цьому важливе значення набувають принципи запобігання збору зайвих даних і ощадливого поводження з інформацією. Це означає, що вибір і структура систем обробки даних повинні бути такими, щоб вони взагалі не обробляли або обробляли якнайменше особистих даних громадян. Негативним прикладом можуть слугувати мобільні телефони, які визначають місцезнаходження абонента в момент початку розмови, хоча тарифи в мережах мобільного телефонного зв'язку не залежать від відстані між учасниками розмови. Тут "принцип найкращого задоволення потреб клієнта поставлений з ніг на голову", – вважає Федеральний уповноважений із захисту даних.

У той же час, цілеспрямоване використання техніки, яка відповідає вимогам захисту даних (*англ. "privacy enhancing technology")*, може значно зменшити загрозу для інформаційного самовизначення окремих громадян. [15] Ця вимога міститься також в опублікованій в 1998 р. доповіді спеціальної комісії Німецького Бундестагу "Майбутнє засобів інформації в економіці і суспільстві – шлях Німеччини в інформаційне суспільство".

В інтересах інформаційної безпеки Федеральний уряд ще в 1991 році створив "Федеральне відомство із забезпечення безпеки в сфері інформаційної техніки" *(нім. Bundesamt fuer Sicherheit in der Informationstechnik)*, яке, крім всього іншого, повинне надавати консультативну допомогу з технічних питань Федеральному уповноваженому із захисту даних [16]. Федеральне відомство повинне також оцінювати безпеку запропонованих на ринку інформаційних систем і, в разі потреби, надавати їм сертифікати безпеки, які можуть ефективно використовуватися в рекламних цілях у сфері електронної торгівлі у ФРН.

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). – http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html. 2. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). – http://europa.eu.int/comm/dg15/en/media/sign/elecsignen.pdf. 3. Informations- und Kommunikationsdienstegesetz. – http://www.iid.de/rahmen/iukdgebt.html. 4. Digital Signature Ordinance. – http://www.iid.de/iukdg/gesetz/sigve.html. 5. Forschung von Baker&McKenzie. – http://www.bmck.com/ecommerce/germany.html. 6. Federal Republic of Germany. Bundesregierung Background Information. – http://www.iid.de/iukdg/gesetz/engindex.html. 7. Federal Republic of Germany. "Signature Law Passes Bundesrat and Can Take Effect Without Delay". – March 2001. – Bundesregierung Background Information. – Germany in the Global Economy. – Fr 2001/03/09. – http://www.iid.de/iukdg/eval/VIB2Referentenentwurfenglisch.pdf. 8. Signaturgesetz. – http://www.gesetze-im-internet.de/sigg_2001/. 9. Forschung von Baker&McKenzie. – http://www.bmck.com/ecommerce/germany.htm. 10. Allgemeine Anforderungen. Signaturgesetz. – http://www.gesetze-im-internet.de/sigg_2001/__4.html. 11. Organisationsstruktur. Regulierungsbehoerde fuer Telekommunikation und Post. – http://www.regtp.de/behoerde/start/in_01-01-00-00-00_m/fs.html. 12. Regulierungsbehoerde fuer Telekommunikation und Post. – http://www.regtp.de/. 13. German Government Position Paper on the International Recognition of Digital Signatures. – http://www.kuner.com/data/sig/gov_digsig_recognition.html. 14. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. – http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html. 15. Privacy-enhancing technologies. – http://en.wikipedia.org/wiki/Privacy_enhancing_technologies. 16. Bundesamt fuer Sicherheit in der Informationstechnik. – https://www.bsi.bund.de/cln_165/DE/Home/home_node.html.

Надійшла до редколегії 12.09.11

М. Безнощенко, канд. екон. наук, доц.

НАСЛІДКИ ВВЕДЕННЯ В УКРАЇНІ ПОДАТКУ НА ДОХОДИ ФІЗИЧНИХ ОСІБ ВІД ДЕПОЗИТІВ

У статті аналізуються можливі позитивні та негативні наслідки введення податку на доходи фізичних осіб від депозитів на економку України. Розглянуто не лише основні якісні зміни, але й наведена кількісна оцінка впливу введення податку на економіку України. В статті розглянута практика оподаткування доходів від депозитів в інших країнах з ринковою економікою.

The article examines the possible positive and negative consequences of introduction of tax on personal income from deposits for the economy of Ukraine. The article considers not only the main qualitative changes, but provides quantitative assessment of impact of the tax on the economy of Ukraine. The article also shows the practice of taxation of income from deposits in other market economies.

Останнім часом, у зв'язку із запропонованим в одному з варіантів Податкового кодексу України введенням оподаткування доходів громадян від депозитів [1], актуальною стала дискусія щодо можливих наслідків такого кроку у фіскальній політиці. В цьому контексті ми вважаємо необхідним проаналізувати можливий вплив цього податку на схильність домогосподарств до заощаджень, на кредитні та депозитні ставки, на доходи державного бюджету і на розвиток економіки в цілому.

Ефекти введення податку на доходи від депозитів є однією з актуальних і все ще недостатньо вивчених тем серед економістів інших, у тому числі розвинених, країн. Слід зауважити, що ця проблематика досить широко обговорюється науковцями всього світу. Дослідження з питань оподаткування індивідуального доходу проводили такі вчені як Беслі Т., Гордон Р., Мертон Р., Менків Г., Міррліс Дж., Потерба Дж., Стігліц Дж. та інші. Серед вітчизняних вчених виділимо таких авторів як Варналій З.С., Данілов О.М., Лисенко В.В., Мельник В.П., Серебрянський Д.М., Тарангул Л.Л., Швабій К.І., Циганов С.А. та інші. Крім того дослідженнями у цій галузі займаються цілі наукові інститути як в Україні так і практично в кожній країні світу. На нашу думку, ретельний попередній аналіз таких ефектів є необхідною передумовою впровадження відповідного податку.

У якості першого кроку в аналізі можливих наслідків введення податку на доходи фізичних осіб від депозитів пропонуємо вивчити ситуацію з оподаткуванням процентного доходу, у тому числі доходів від депозитів у інших країнах світу та розглянути основні аргументи на користь та проти введення такого податку.