

Стрельцов Л.Є.

*Інститут зарубіжного та міжнародного кримінального права
імені Макса Планка (ФРН),
дослідник, кандидат юридичних наук*

КОМП'ЮТЕРНІ ЗЛОЧИННИ У КРИМІНАЛЬНОМУ ПРАВІ ФРН

Кримінальне право, як вважається у Федеративній Республіці Німеччини (далі – ФРН), є засобом здійснення кримінальної політики, і воно нормує напрямки боротьби зі злочинністю. На сучасному етапі ця політика характеризується двома основними тенденціями: по-перше, застосуванням суворих покарань до осіб, що чинять тяжкі злочини або неодноразово порушують кримінальний закон, і, по-друге, звуженням сфери кримінальної відповідальності за злочини, які не є «дійсно» суспільно небезпечними.

Загалом структура кримінального законодавства ФРН включає: Конституцію ФРН 1949 року, Кримінальний кодекс Німеччини 1871 року (з усіма змінами та доповненнями), спеціальні федеральні кримінальні закони, кримінальне законодавство земель, іноземне кримінальне законодавство. Таким чином, кримінальне право ФРН не є повністю кодифікованим. Тому слід розрізняти власне Кримінальний кодекс ФРН (федеральний кодифікований акт) і більш широке поняття – «кримінальне право», яке включає і КК ФРН, і інші кримінально-правові приписи різних законів, що становлять так зване додаткове кримінальне право.

Зміни, які відбуваються сьогодні в інформаційній сфері, вимагають і відповідної уваги з боку кримінального права, положення якого повинні виділити ті суспільно небезпечні діяння, які порушують функціонування цієї сфери, і встановити за їх вчинення відповідні кримінально-правові заходи.

З огляду на те, що комплексність і багатоаспектність інформаційної сфери заслуговує на спеціальну увагу (див.: Lev Streltsov. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. European Journal for Security Research. November 2017, Volume 2, Issue 2, pp. 147-184), в тому числі і в плані її правового регулювання та правової охорони, зупинимося в цій публікації тільки

на одному напрямку: комп'ютерних злочинах.

На відміну від кримінального права України в Особливій частини німецького кримінального права не виділений окремий розділ (група) таких злочинів. Німецький законодавець пішов іншим шляхом. Так, законом ФРН «Про боротьбу з економічною злочинністю» від 15 травня 1986 р.у Кримінальний кодекс ФРН було включено цілий ряд норм, що формулюють нові склади злочинів, які повинні охопити найбільш часто вчиняємі і найбільш небезпечні склади злочинів у сфері використання комп'ютерів. Вони були включені у вигляді додаткових параграфів: § 202-а (Дії, спрямовані на отримання відомостей), § 263-а (Комп'ютерне шахрайство), § 303-а (Зміна даних), § 303-6 (Комп'ютерний саботаж). Ще один склад – підробка даних, що мають доказове значення, був включений в КК ФРН шляхом редакції (внесення змін) § 269.

Дії, спрямовані на отримання відомостей (§ 202-а), на практиці називають незаконним вивідування комп'ютерних даних (комп'ютерне шпигунство). Сутність його полягає в тому, що особа незаконно (тобто не маючи на те повноважень) здобуває собі або для кого-небудь іншого комп'ютерні відомості, «які йому не призначаються і особливо охороняються».

Комп'ютерне шахрайство (§ 263-а КК ФРН) визнається найбільш небезпечним з групи комп'ютерних злочинів. Винним в ньому вважається той, хто з наміром отримати матеріальну вигоду для себе або іншої особи заподіює шкоду майну потерпілого, впливаючи на результати обробки даних шляхом неправильного створення програм, використання неправильних або неповних даних, неправомірного застосування даних або іншого неправомірного впливу на результат їх обробки.

До комп'ютерного шахрайства близьким за своєю природою є злочин, передбачений § 269 КК ФРН, – підробка даних, що мають доказове значення. Відповідно до роз'яснення, що міститься в новій редакції § 270 КК ФРН, «до обману в правозастосовчій діяльності прирівнюється фальсифіковане використання результатів переробки даних у правозастосовчій діяльності». Це роз'яснення важливе для випадків, коли фальсифікація комп'ютерних даних досягається без безпосереднього обману людини, зайнятої їх обробкою.

Певною мірою окремо розташовані два склади злочинів, які умовно

можна назвати «технічними». Вони знаходяться в розд. 27 «Пошкодження майна» КК ФРН. Зміна даних (§ 303-а КК ФРН) – це протиправне анулювання, знищення даних, приведення їх у непридатність або їх зміна. Комп’ютерний саботаж (§ 303-6 КК ФРН) – це порушення обробки даних, що мають істотне значення для чужого підприємства, організації чи органу шляхом: 1) вчинення діяння, передбаченого в § 303-а КК ФРН; 2) руйнування, пошкодження, приведення в непридатність, усунення або зміни установки для обробки даних або носія інформації.

Слід підкреслити, що незважаючи на досить серйозну небезпеку обох названих злочинів, кримінальне переслідування за них можливо тільки за скаргою потерпілого (переважно їм є юридична особа), за винятком окремих випадків, вказаних у законодавстві.

Проведений аналіз свідчить, що законодавство про кримінальну відповідальність за комп’ютерні злочини в ФРН має певні особливості. Але українському законодавцеві буде корисним, як здається, оцінити німецький досвід для подальшого підвищення боротьби з комп’ютерними злочинами вже на своїх теренах.